Security Administration Handbook

Version 10

July 26, 2010

Table of Contents

Important Information Please Read

GRIEVANCE USER – Access via the Portal - Authorization for BI Reports

CLIENT	USER ACCOUNT	ROLES
RP0	8-digit Pernr account	SR3P_DE_GRIEVANCE_ADMIN or SR3P_DE_GRIEVANCE_INQ
BIP	8-digit Pernr account	ZS_BI_XXXX_END_USER (XXXX is 4 or 5 digit agency number) ZS_BI_XXXX_WBWT ZS_BI_SOW_WBWT ZS_BI_GENERAL_ACCESS ZS_BI-GR_ANALYSIS (Infocube role)
	Notes: If this is an existing BI User who has a POWER_USER or END_USER role, you only need to add the ZS_BI-GR_ANALYSIS role. Depending on other requirements, the user may also have FI and/or HR roles. Centralized Grievance roles are handled by DOP.	
HRMS PORTAL	Professional UserID – LDAP or UME	BI_REPORTS_GRP
	Map the Professional User account to their BIP Pernr UserID You MUST also contact the DOP Service Center to have Professional Portal accounts mapped to the Federated Portal	

DECENTRALIZED SECURITY ADMINISTRATORS

CLIENT	USER ACCOUNT	ROLES
RP0	8-digit Pernr account Add entry in the OOSB (T77UA) with the appropriate authorization data profile	SR3P_XXXX_USER_ADMIN and/or SR3P_XXXX_AUTH_ADMIN
BIP	8-digit Pernr account	ZS_BI_XXXX_ USER_ADMIN ZS_BI_GENERAL_ACCESS
HRMS PORTAL	Professional UserID – LDAP or UME	User Admin Role on the Assigned Roles tab

Checklist for UserID Account Maintenance

This checklist outlines what is required in each of the systems in order for a professional user to have appropriate access in the Human Resource Management System. This also outlines the steps to complete on professional and non-professional user accounts when employees transfer to other agencies or are withdrawn from state employment.

I. **HCM Professional Users**
- Roles assigned to the position in HCM
- SU01 User Account with validity dates and Agency User Group
- >For SSO Users ONLY: Entry in SNC tab

  Note: Effective April 27, 2010 agency Security Administrators will no longer need to assign licenses in SU01. Licenses are assigned automatically to the user account based on the roles assigned.
- Entry of Authorized Profile in OOSB
  - If PERS_ADMIN_PROC role is assigned add additional entry of WA_SOW in OOSB

II. **BI Professional Users**
- Roles assigned in BI
- SU01 User Account with validity dates and Agency User Group
- >For SSO Users ONLY: Entry in SNC tab
- Entry of Authorized Profile in OOSB in HCM

  Note: Effective April 27, 2010 agency Security Administrators will no longer need to assign licenses in SU01. Licenses are assigned automatically to the user account based on the roles assigned.

III. **Portal Professional Users**
- Email address (LDAP) or agency domain\username (UME) UserID account
- BI Reporting for Grievance, HR or Finance :
  - SU01 User Account with validity dates (HCM – Section I)
  - Entry of Authorized Profile in OOSB (HCM –Section I)
  - SU01 User account with role(s) and validity dates in BI (BI - Section II)
  - BI_Reports_GRP role assigned to the Professional portal account
  - Professional Portal account mapped to user's BI account

    ***Effective April 26, 2010 you MUST also contact the DOP Service Center to have Professional Portal accounts mapped to the Federated Portal.*
- WEBGUI users
  - Roles assigned to the position in HCM (HCM – Section I)
  - SU01 User account with General_Access role and validity dates in BI (BI - Section II)
  - HR_HTMLGUI_GRP role assigned to the Professional portal account
  - Professional Portal account mapped to user's BI account

    ***Effective April 26, 2010 you MUST also contact the DOP Service Center to have Professional Portal accounts mapped to the Federated Portal.*

When Employees Transfer out of the Agency (Professional Users Only)

- HCM – Delete employees profile entries in OOSB
- HCM – Change the User Group back to ESSUSER in SU01
- HCM – Delete the SNC entry – SSO only
- BI – Delete the BI user account
- Portal – Delete user mapping for agency Domain\Username – UME Professional account
- Portal – Delete the Professional account (agency Domain\Username - UME) - LDAP e-mail address account cannot be deleted
- Portal – Delete the Group and/or User_Admin roles (LDAP)
- Portal – Delete user mapping for e-mail address account (LDAP)

  ***Effective April 26, 2010 you MUST also contact the DOP Service Center to have Professional Portal accounts mapping cleared from the Federated Portal.*

When Employees Leave State Employment – Withdrawn Status (Professional and Non-Professional Users)

- HCM – Delete profile entries in OOSB if there are entries
- HCM – Delete the user account (SU01) – this takes away user's access to ESS
- BI – Delete the BI user account if created
- Portal – Delete the ESS account (8 digit personnel number - UME)
- Portal – Delete user mapping for agency Domain\Username – UME Professional account

  ***Effective April 26, 2010 you MUST also contact the DOP Service Center to have Professional Portal accounts mapping cleared from the Federated Portal.*
- Portal – Delete the Professional account (agency Domain\Username - UME) LDAP e-mail address account cannot be deleted
- Portal – Delete the Group and/or User_Admin roles from the e-mail address account (LDAP)
- Portal – Delete user mapping for e-mail address account (LDAP)

  ***Effective April 26, 2010 you MUST also contact the DOP Service Center to have Professional Portal accounts mapping cleared from the Federated Portal.*

SAP License Assignment Matrix

Note: Effective April 27, 2010 agency Security Administrators will no longer need to assign licenses in SU01. Licenses are assigned automatically to the user account based on the roles assigned. License information will no longer show in SU01, in the LicenceData Tab. **This matrix is for reference only.** If you have questions about licenses please contact the DOP Service Center at 360-664-6400 or servicecenter@dop.wa.gov.

HCM (RP0)

Column A	Column B	Column C
mySAP Business Suite Professional	**mySAP Business Suite Limited Professional**	**mySAP Business Suite Employee**
SR3P_XXXX_AUTH_ADMIN SR3P_XXXX_USER_ADMIN SR3P_CE_GRIEVANCE_ADMIN SR3P_CE_OST_PAYOPS_ADMIN SR3P_CE_SECURITY_AUDIT SR3P_DE_BENE_PROC SR3P_DE_GARNISH_ADMIN SR3P_DE_GRIEVANCE_ADMIN SR3P_DE_FIN_RPT_PROC SR3P_DE_LEAVE_CORR_PROC SR3P_DE_ORG_MANG_PROC SR3P_DE_PAY_ANL SR3P_DE_PAY_PROC SR3P_DE_PAY_SUPV SR3P_DE_PERS_ADMIN_PROC SR3P_DE_PERS_ADMIN_SUPV SR3P_DE_QUALADM SR3P_DE_T&A_PROC SR3P_DE_T&A_SUPV and SR3P_SOW_ESS	SR3P_XXXX_DATA_PROFILE SR3P_XXXX_SECURITY_AUDIT CR3P_CE_INQ_HELP_DESK SR3P_CE_BENEFITS_INQ SR3P_CE_GARN_INQ SR3P_DE_GRIEVANCE_INQ SR3P_DE_ORG_MGT_INQ SR3P_DE_PAY_INQ SR3P_DE_PERS_ADMIN_INQ SR3P_DE_T&A_INQ and SR3P_SOW_ESS	SR3P_SOW_ESS

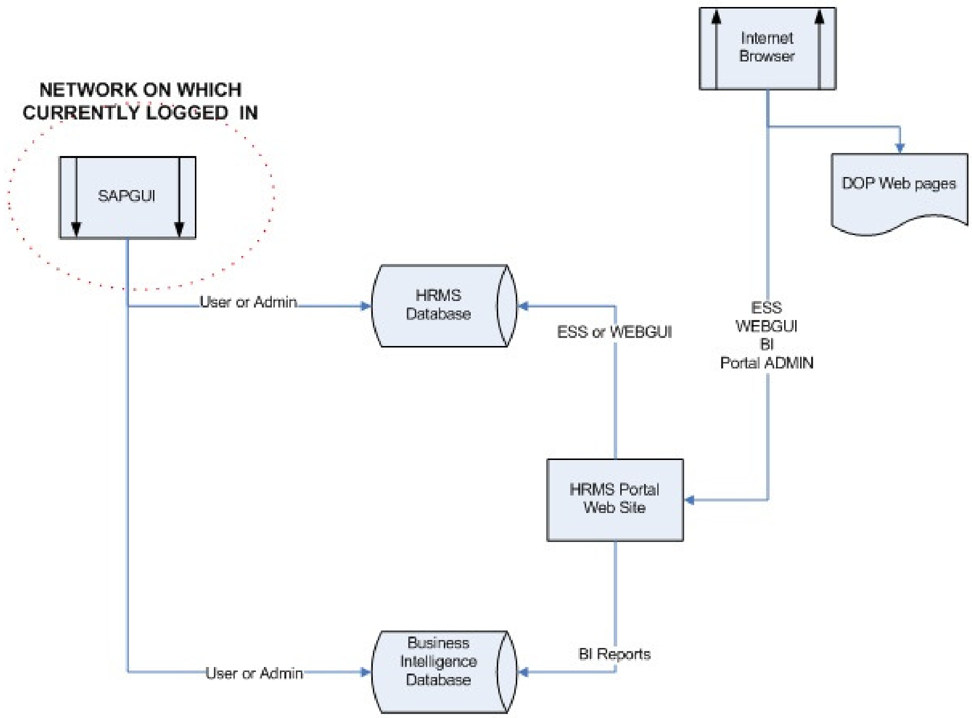
Business Intelligence (BIP)

Column A	Column B
mySAP Business Suite Professional	**mySAP Business Suite Limited Professional**
ZS_BI_XXXX_USER_ADMIN ZS_BI_XXXX_POWER_USER	ZS_BI_XXXX_END_USER ZS_BI_XXXX_SECURITY_AUDIT ZS_BI_XXXX_WBWT ZS_BI_GENERAL_ACCESS ZS_BI_SOW_WBWT ZS_BI-FI_ANALYSIS ZS_BI-FI_SOW_ANALYSIS ZS_BI-GR_ANALYSIS ZS_BI-GR_SOW_ANALYSIS ZS_BI-HR_ANALYSIS ZS_BI-HR_SOW_ANALYSIS

Systems Overview

As a Human Resource Management System (HRMS) Security User or Authorization Administrator, you will be responsible for assisting your agency professional staff interface with the DOP HRMS.
HRMS consists of: Human Capital Management (HCM), Business Intelligence (BI) and Enterprise Portal (HRMS Portal)

The chart below shows all of the systems and how they are accessed in very general terms:



The "SAPGUI" noted at the top left of the diagram is a Desktop application entry point. If your agency works within the State Government Network (SGN), the SAPGUI gives you a "stateful" connection to the following applications:

- HCM database of Personnel and Payroll information
- Business Intelligence (BI) - previously called "Business Warehouse (BW)"

If you are in a K-20 system or the Military system or otherwise OUTSIDE the SGN, specific arrangements can be made with DOP or DIS in order for your agency to access the HRMS systems.

The HRMS Portal is an alternative method of entering the various systems using a professional portal UserID (LDAP or agency UME).
The HRMS Portal is the ONLY way to enter Employee Self Service (ESS) using an 8 digit pernr.

The HRMS Portal is available for access from outside the SGN via the internet - https://wahrms.wa.gov/irj/portal

The HRMS Portal is available for access from inside the SGN via the internet - https://myhrms.wa.gov/irj/portal

General Naming Conventions

There are several parts/nodes to the role names in the HRMS. The following is the explanation of each node:

- The First Node identifies whether the role is a “**S**”ingle role or “**C**”omposite, “**R3**” and that it is a “**P**”roduction role
  - Single roles will begin with “**S**”
  - Composite roles (roles made up of single roles) will begin with “**C**”
  - HCM (old R3) Roles will have “**R3**” as the second and third characters in the role name.
  - The fourth character will be “**P**” identifying the role as a production role.
- The Second Node identifies whether the role is (“**DE**”centralized or “**CE**”ntralized) or custom
  - Decentralized roles and “SR3P_SOW_ESS” may be assigned by agency Authorization Administrators.
  - Centralized and custom roles may only be assigned by DOP.
- All subsequent Nodes describe the intended role function.
  - Example: SR3P_DE_PAY_ANL – Decentralized Payroll Analyst, built as single role and assignable by agencies.
- BI roles begin with ‘ZS_BI*’ the remaining characters being as descriptive as possible to match the role name.
  - Example: ZS_BI _1110_USER_ADMIN – BI User Administrator for a particular agency.

HCM Roles

HCM Professional user accounts generally consist of at least one Decentralized Role or Centralized Role and a Structural Data Profile Role.

Security Admin, Auth and Audit Professional user accounts consist of at least one Security/Auth/Audit Role and a Structural Data Profile Role.

- Decentralized HR Roles begin with ‘SR3P_DE*’ with the remaining characters being as descriptive as possible to match the role name.
  - Example: SR3P_DE_PAY_ANL – Decentralized Payroll Analyst
- Centralized HR Roles begin with ‘SR3P_CE*’ with the remaining characters being as descriptive as possible to match the role name.
  - Example: SR3P_CE_FINC_APRV – Centralized Financial Approver
- Security Admin and Auth Roles begin with ‘SR3P_XXXX*’ with the remaining characters being as descriptive as possible to match the role name, and XXXX being the Personnel Area/Agency.
  - Example: SR3P_1110_AUTH_ADMIN – DOP Authorization Administrator
- Structural Data Profile Roles begin with ‘SR3P_XXXX_DATA_PROFILE’ with XXXX being the Personnel Area/Agency.
  - Example: SR3P_1110_DATA_PROFILE – DOP Structural Profile Role
- Security Audit Roles consist of Decentralized SR3P_XXXX_SECURITY_AUDIT or SR3P_CE_SECURITY_AUDIT.

NOTE: ***All Centralized roles are assigned by DOP.***

User Groups in HCM and BI

- User Groups are formatted as follows: WA_XXXX
  - Where XXXX = Personnel Area/Agency

- The description should match the agency name (example follows)
  - User Group: WA_1110
  - Description: Department of Personnel

BI Roles

BI professional users are required to have an HCM UserID account with an agency Data Profile Role assigned to their position and the agency authorization profile entered in the OOSB, before creating the BI UserID account.

BI Professional user accounts include:

- one End or Power User role – ZS_BI_XXXX_POWER_USER / ZS_BI_XXXX_END_USER
- one or more of the InfoCube Roles – ZS_BI-FI_ANALYSIS, ZS_BI-HR_ANALYSIS, ZS_BI-GR_ANALYSIS
- agency and statewide Workbook/Web Template Roles – ZS_BI_XXXX_WBWT and ZS_BI_SOW_WBWT
- the General Access role – ZS_BI_GENERAL_ACCESS

- BI End User, Power User, and Workbook/Web Template Roles begin with 'ZS_BI_*' and Personnel area with the remaining characters being as descriptive as possible to match the role name.
  - Example: ZS_BI_1110_END_USER – DOP BI End User

- BI InfoCube Roles (HR, FI, or GR) begin with 'ZS_BI -*' with the remaining characters being as descriptive as possible to match the role name.
  - Example: ZS_BI-FI_ANALYSIS
ZS_BI-FI_SOW_ANALYSIS
ZS_BI-HR_ANALYSIS
ZS_BI-HR_SOW_ANALYSIS
ZS_BI-GR_ANALYSIS
ZS_BI-GR_SOW_ANALYSIS

- Security Admin Roles begin with 'ZS_BI _XXXX*' with the remaining characters being as descriptive as possible to match the role name, and XXXX being the Personnel Area/Agency.
  - Example: ZS_BI _1110_USER_ADMIN – DOP UserID Administrator for BI

Portal Roles

Portal Roles include:

- Portal User Admin – Single role
- BI_Reports_GRP – Group role – Accessing BI Reports through the HRMS Portal.
- HR_HtmlGui_GRP – Group role – Accessing HRMS through the HRMS Portal
- ESS_ GRP – Group role – Accessing Employee Self Service

HCM Authorization Administrator SR3P_XXXX_AUTH_ADMIN

Introduction

Security within the HRMS is based on a record called a “UserID”. A UserID is necessary to enter a specific system within the HRMS. It is distinct and separate from personnel records and is the primary responsibility of the UserID Administrator. Things like name changes in the personnel/payroll records do NOT propagate to the UserID records.

Each UserID may be assigned Professional Roles which define how the user will interface with the specific system within the HRMS. In the Personnel/Payroll system (aka HRMS, R3 or HCM) Professional roles are divided into the following areas:

- Personnel
- Payroll
- Time & Attendance
- Grievance
- Organizational Management
- Security Administration

In each of those functional areas, there are tiers of access:

- “Processor” or “Administrator” levels have the most authority to update Master Data;
- “Inquiry” roles, which can view Master Data, cannot update it.
- “Supervisor” roles have some qualities of both Processors and Inquirers.

There are other roles available in the system, but decentralized agency authorization administrators only have the authority to assign roles available to their agencies.

Dept. of Personnel Setup for Non-Professional UserID accounts

1. DOP creates UserID for new hires (SU01)
2. DOP links Personnel Record to UserID (PA30)
3. DOP assigns the SR3P_SOW_ESS role
4. DOP creates ESS Portal accounts for new employees
5. DOP distributes ESS passwords to User Administrators

NOTE:

- New employee UserIDs are created by DOP twice weekly. DOP creates Employee Self Service UserIDs (Pernr-based) in the Portal. These ESS Portal accounts have access to ‘Personal Information’ and ‘Earning Statements’.

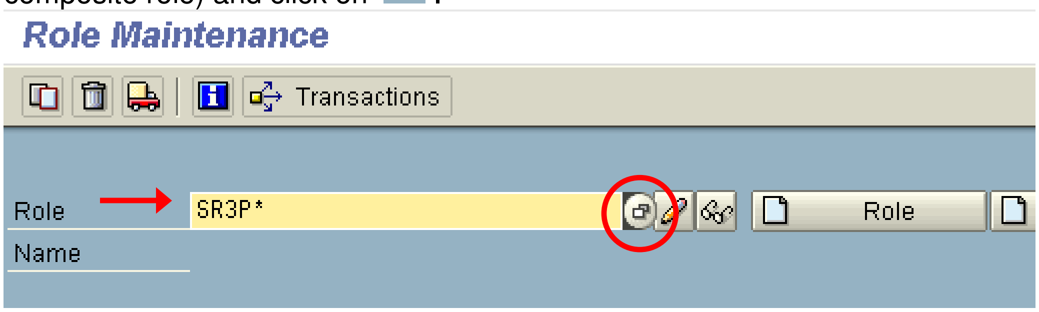
Assign Roles to Positions Using PFCG

Prerequisites:
- ✓ Role name(s)
- ✓ SAP position number(s).

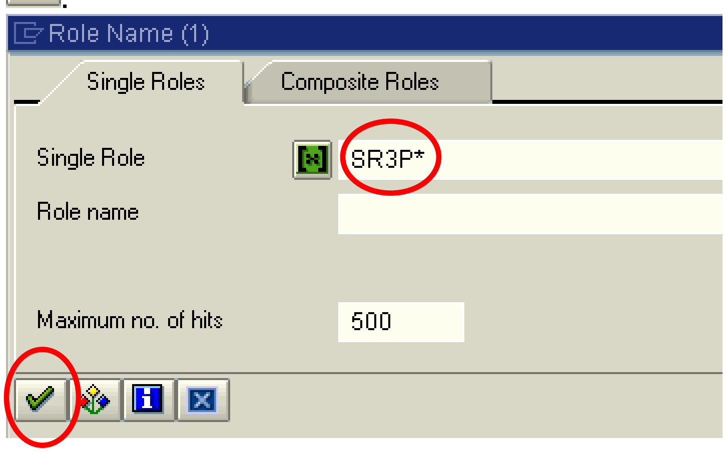
NOTE: *To quickly find the position number, do the following:*
PA20 → Enter Personnel number → Select Actions → Display → the position number will be under Organizational Assignment block in the middle of the screen. Copy the position number and continue with the Role Assignment steps below.

1. Enter transaction '**PFCG**' (/nPFCG) to assign roles to positions.

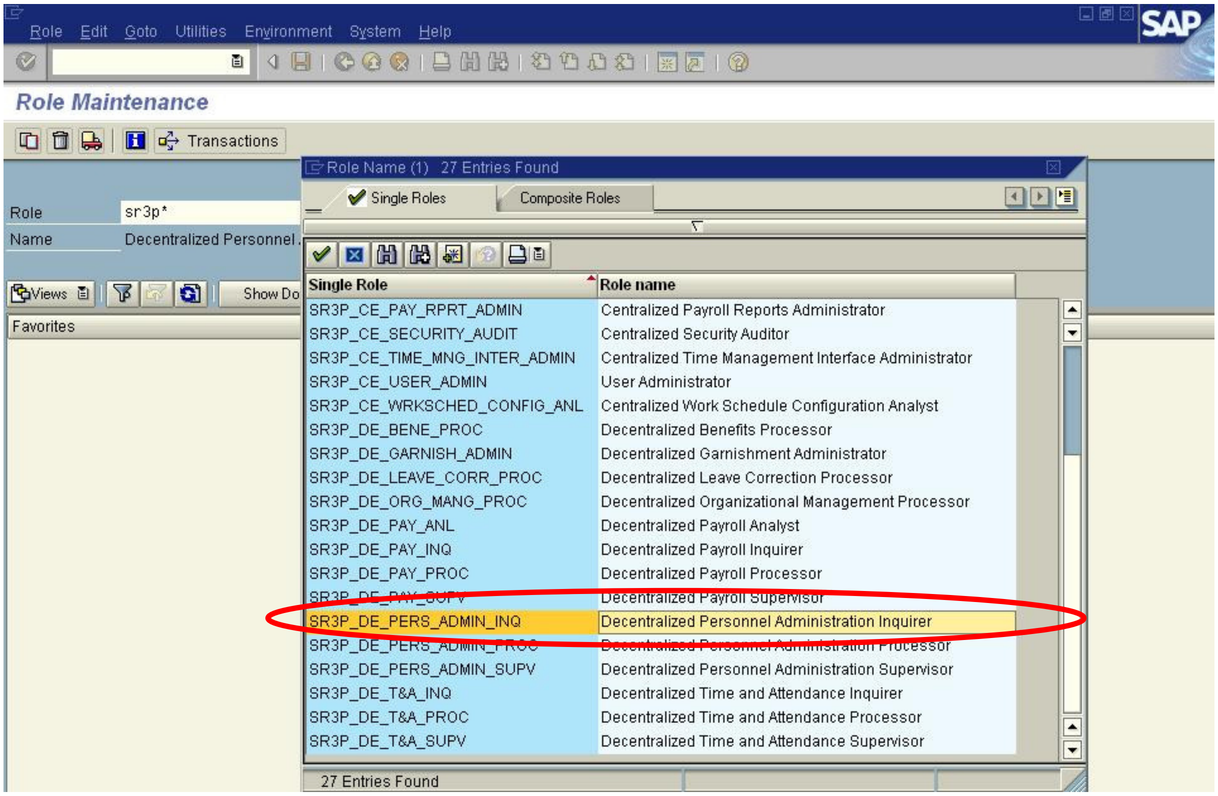
2. If you know the fully qualified role name, enter it in the 'Role' field, and skip to Step 5. Otherwise, search for a role that needs to be assigned to a position. Key SR3P* (for single role) or CR3P* (for composite role) and click on  .



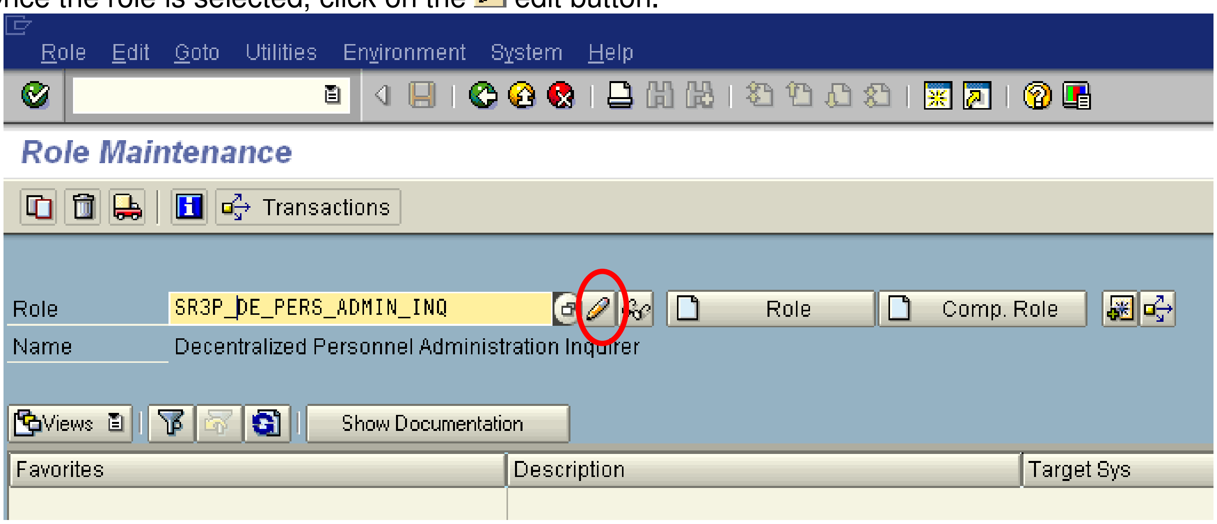
3. Verify/confirm the proper tab ('Single Roles' for SR3P*; 'Composite Roles' for CR3P*) and click on  .



4. Double click on the appropriate role; for this example, 'Personnel Administration Inquirer' is selected.

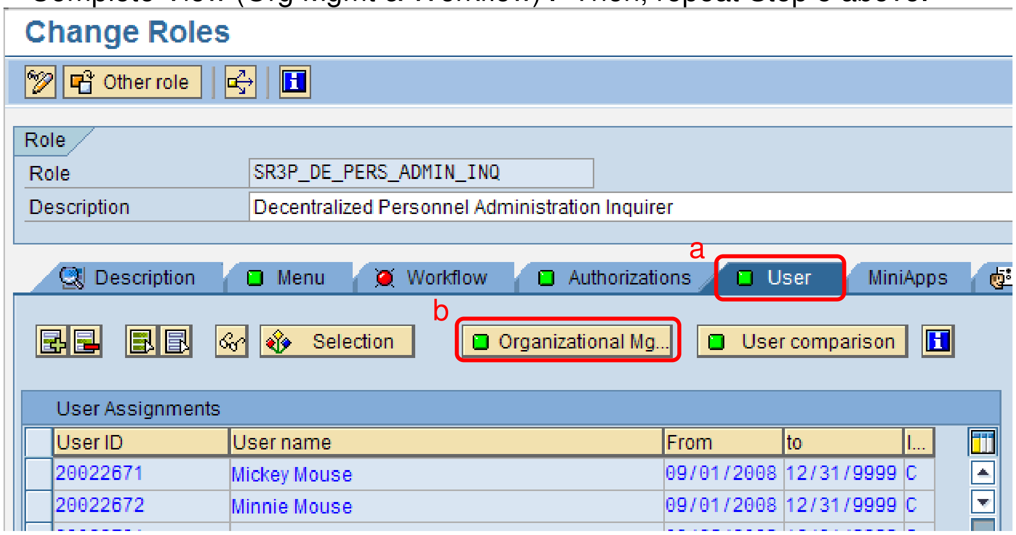


5. Once the role is selected, click on the edit button.

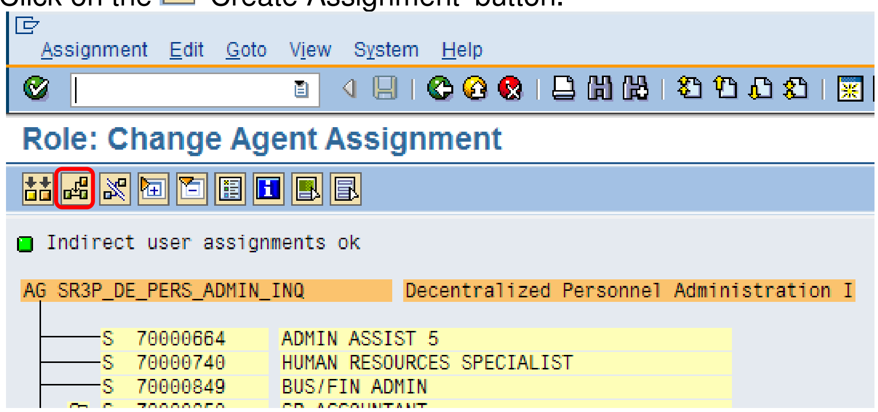


a. Click on the ‘User’ tab

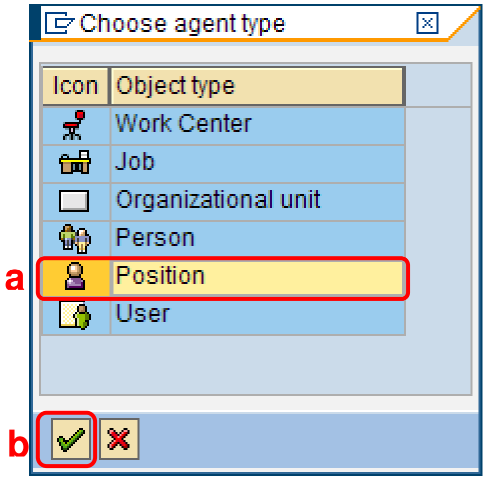
b. Click on the “Organizational Mg…” button. **IF this button does not appear**, click on the  ‘back’ button, then click ‘Goto’ pull-down menu (on menu bar), select ‘Settings” and select ‘Complete View (Org Mgmt & Workflow)’. Then, repeat Step 5 above.



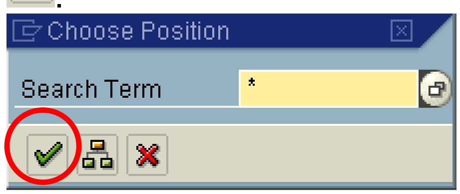
6. Click on the  ‘Create Assignment’ button.



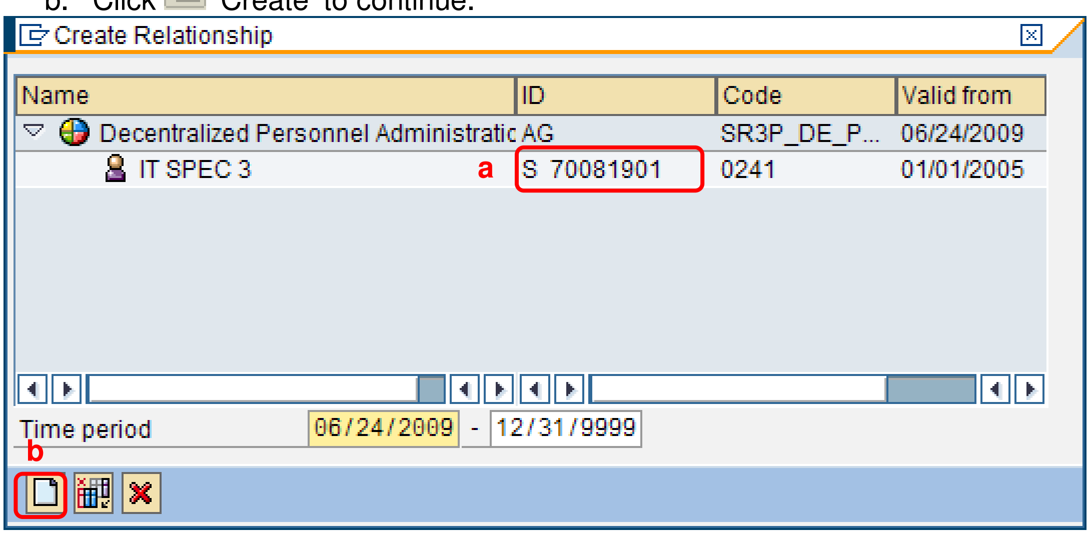
7. Choose agent type
   a. Click on 'Position' as the object type
   b. Click the 'enter' button.



8. Enter SAP position number (w/o the 'S') in 'Search Term' field (overlay/replace the *), and click on .

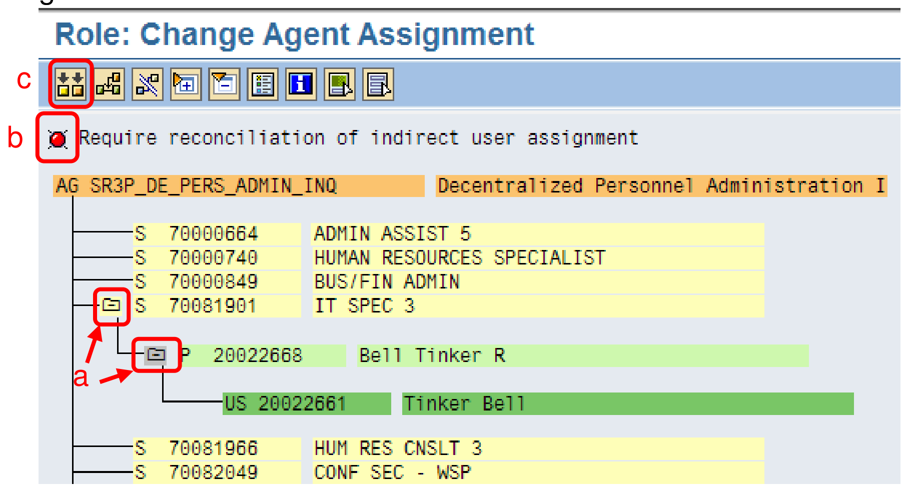


9. The appropriate role and position should be displayed.
   a. Confirm/verify SAP Position number is correct.
   b. Click 'Create' to continue.

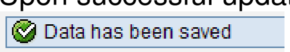


Reconcile the Roles Using PFCG

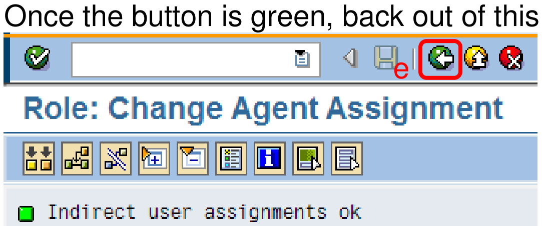
10. The position should now be displayed.
    a. Click on the to drill down within the position to make sure that it contains the correct person and the UserID.
    b. Notice that there is a red button at the top of the screen.
    c. Click on 'Indirect user assignment reconciliation' button and the button should then turn green



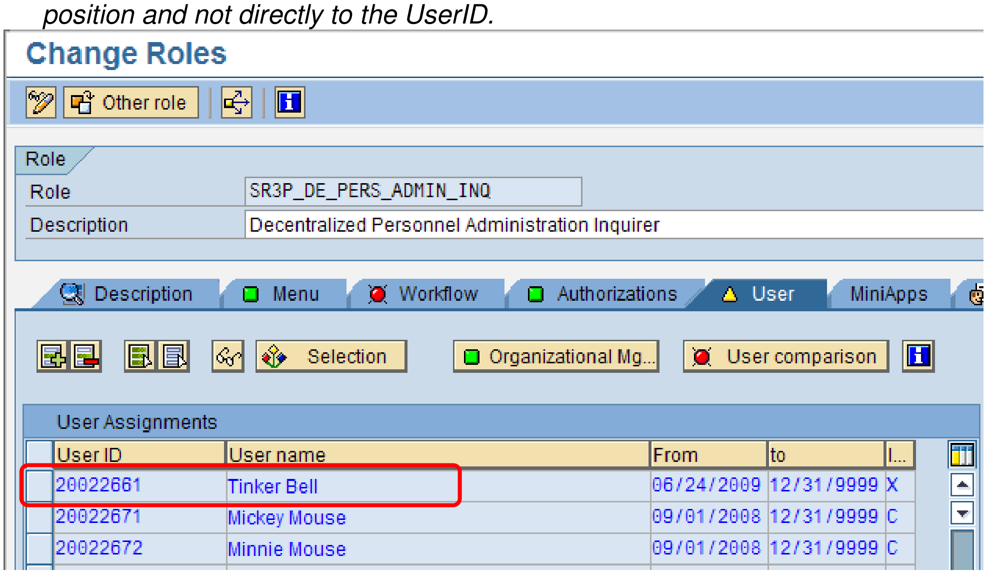
    d. Upon successful update you will see the following message in the status area:



    e. Once the button is green, back out of this screen.



11. The UserID and user name should now be included in the list, in blue.
    NOTE*: Blue means the employee has roles assigned by position. You should always assign roles to position and not directly to the UserID.*

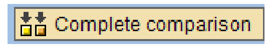


12. If the 

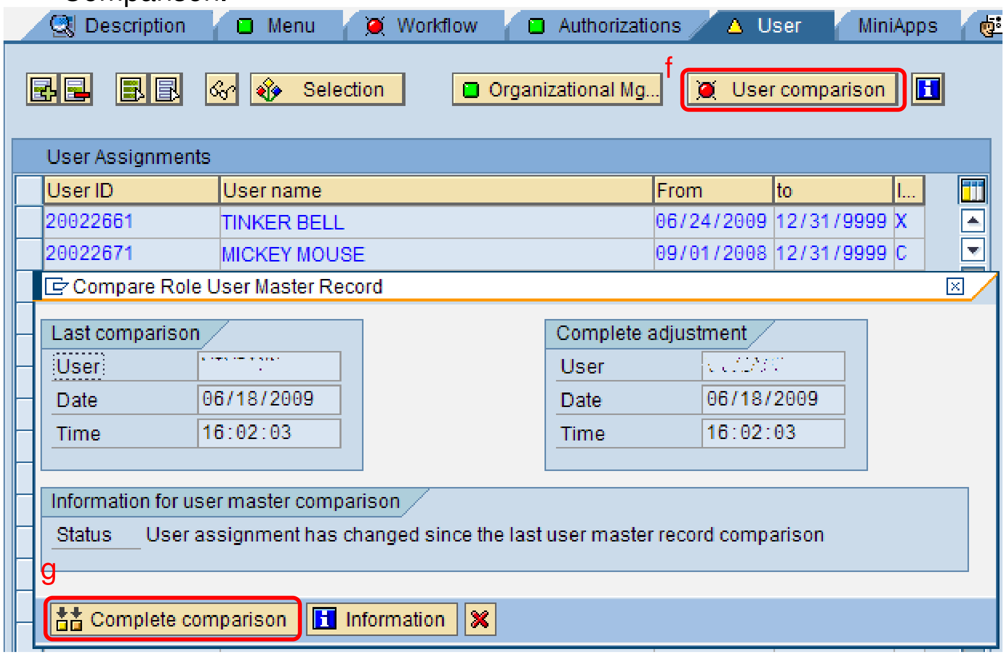
'User comparison' button is red,

   f. Click on the 

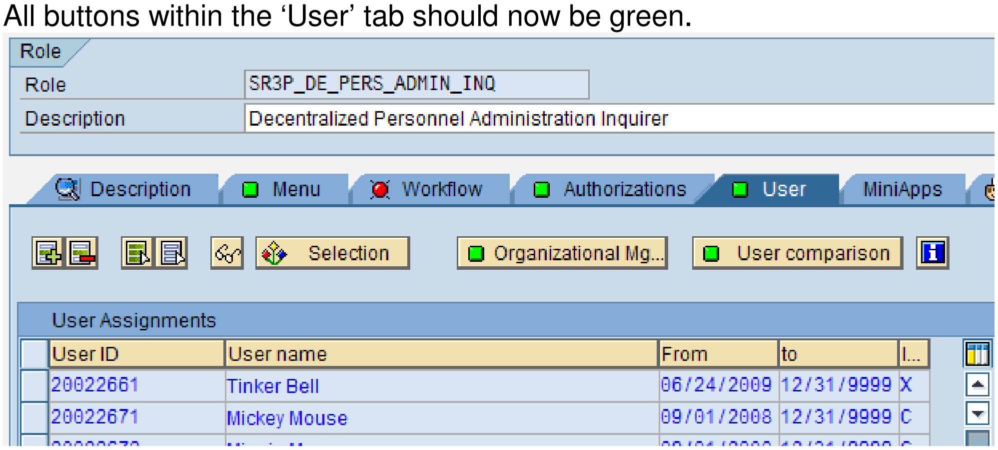
button

   g. In the Compare Role User Master Record popup, click on 

'Complete Comparison.'



13. All buttons within the 'User' tab should now be green.



14. Click the 'Save'  button to save changes to the role.

15. Follow the same steps for **[Assign Roles to Positions (PFCG)]** to assign the agency Data Profile role with the following naming convention: SR3P_**XXXX**_DATA_PROFILE – where XXXX is your Personnel Area.
16. Contact your User Administrator after all roles are assigned, they need to go to SU01 and [complete the steps for maintaining a professional user.]

Assign Roles to Positions Using PPOMW

NOTE: *PPOMW transaction lets you assign multiple roles at once.*

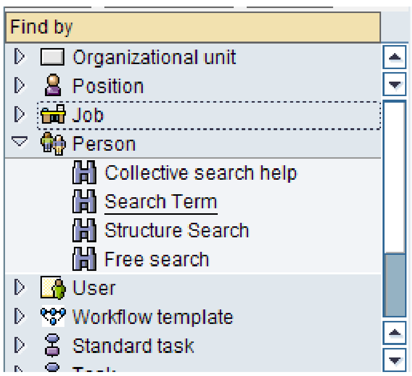
Prerequisites:
✓ User's name or
✓ Users UserID/Personnel Number (8 digits) or
✓ SAP Position number
NOTE: *You must always assign roles to positions.*

1. Enter transaction '**PPOMW**' (/nPPOMW). You will see 

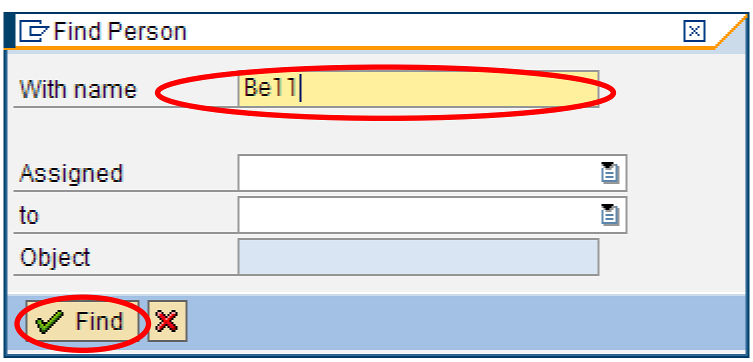
in the status area. Disregard this message and continue.

Find the position number

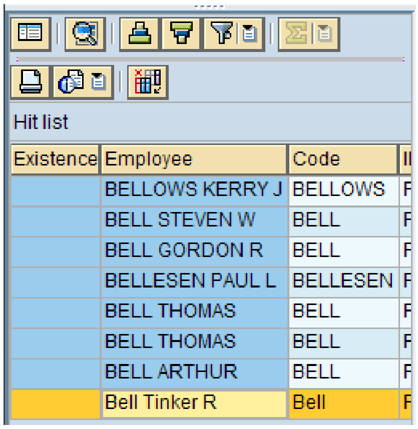
2. Search for position(s). Click on the  button next to 'Person'.



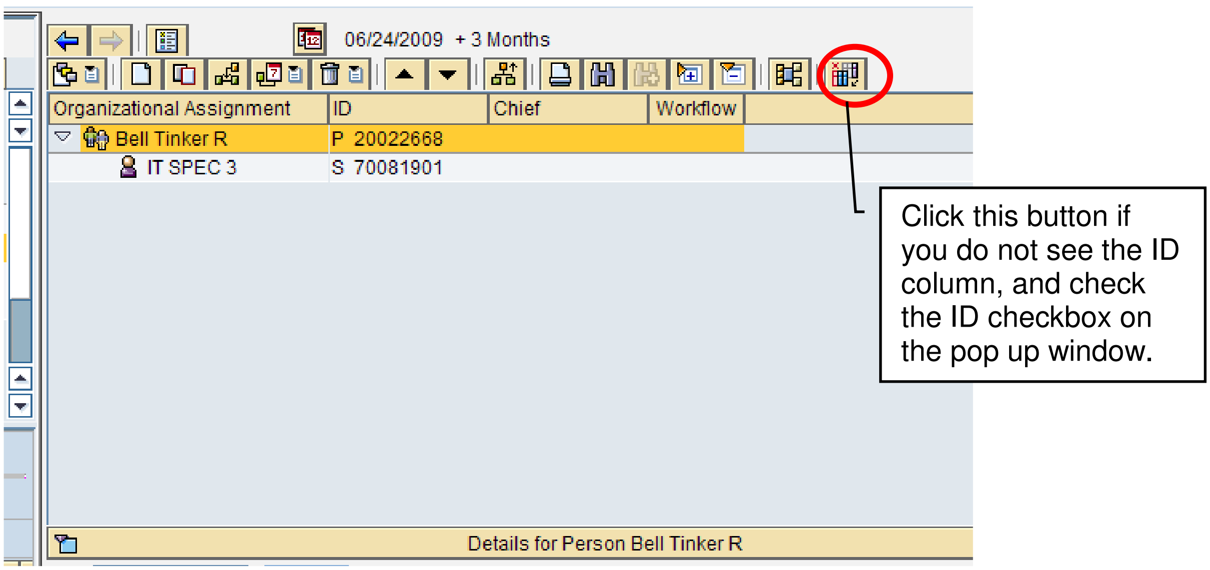
3. In the expanded display, click on the 'Search Term' and fill the resultant "With Name" box with EITHER the person's last name or the person's Pernr. Click the Find Icon.



4. Double click on the desired name…

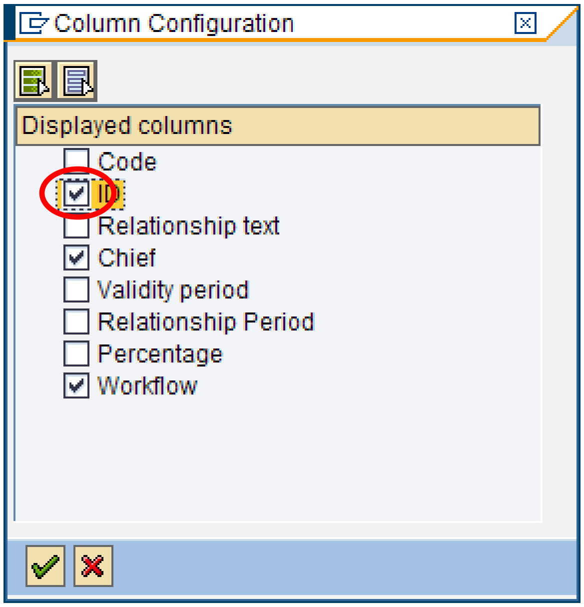


5. …and the Position number shows as the "S" entry under the "ID" column (In the upper right screen quadrant). Verify correct employee.



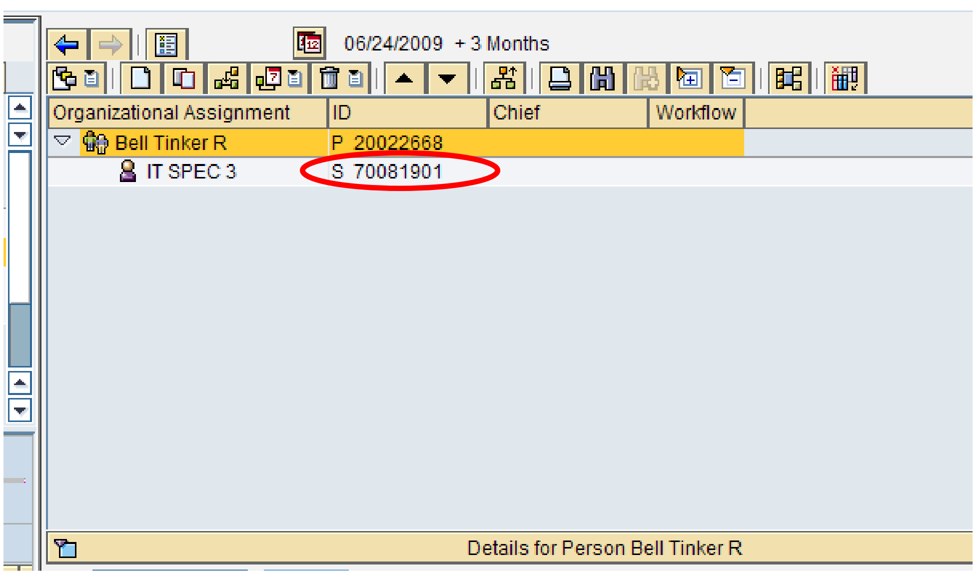
Add the ID column

(If your presentation doesn't show you an ID column, click on the "columns" icon in the box circled in red above. A popup box as shown below will allow you to select columns. Put a checkmark in the "ID" box and click the green checkmark icon in the lower left.)

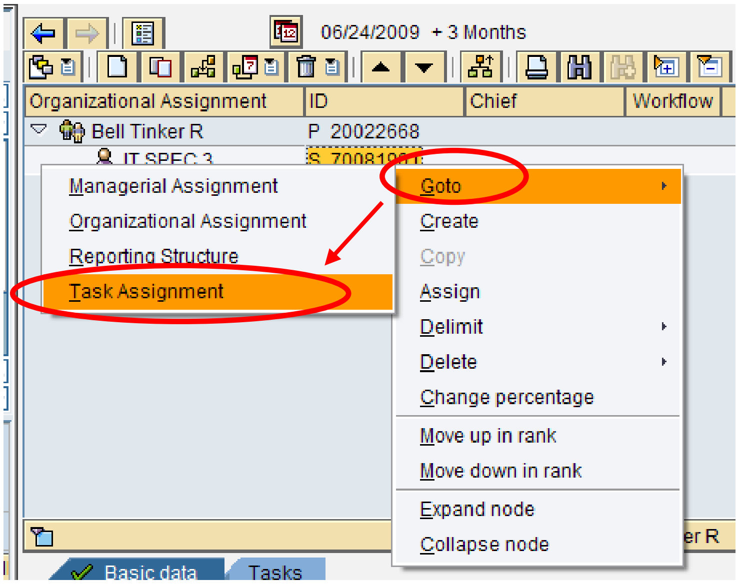


Show currently assigned roles

6. On the information screen shown here, right click on the position number…

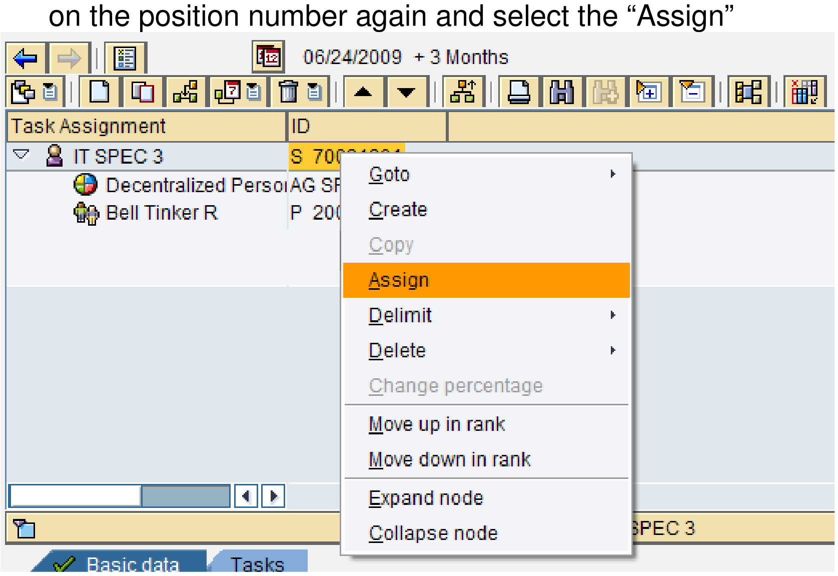


7. Highlighting the resultant “Goto” option will extend a box which allows you to select and click on “Task Assignment” as shown here.

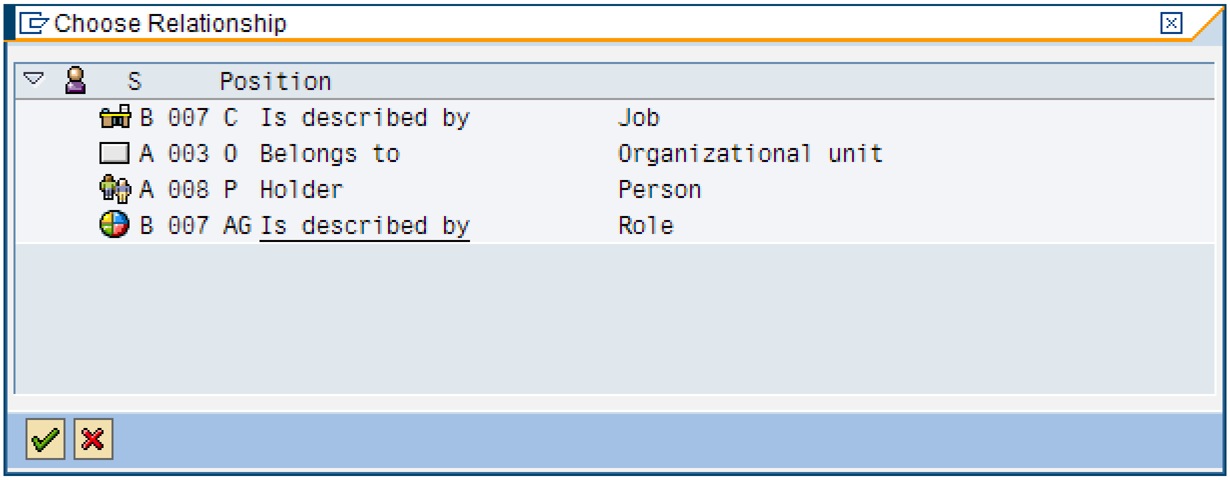


Add roles

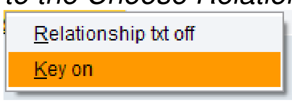
8. This will show you all the professional roles assigned this Position number. To add more, right click on the position number again and select the “Assign”



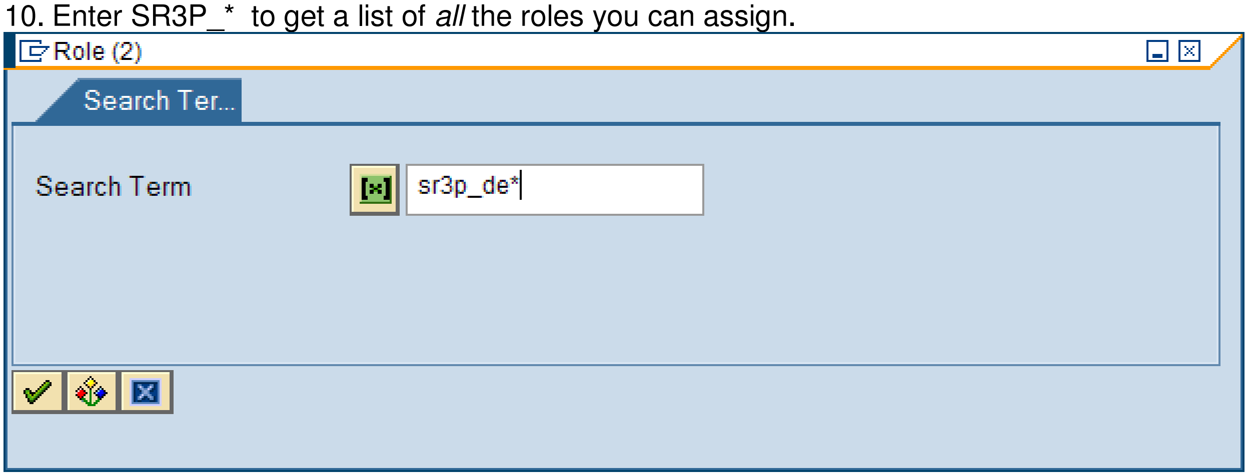
9. “Role” relationships can be assigned by double clicking on the bottom line (Is described by Role) shown here.. (or click the bottom line, then the green arrow…)



NOTE: *If you don't see the technical names such as AG next to the Is described by, go back to step 8, to the Choose Relationship screen. Right click anywhere on the screen and click on Key on.*

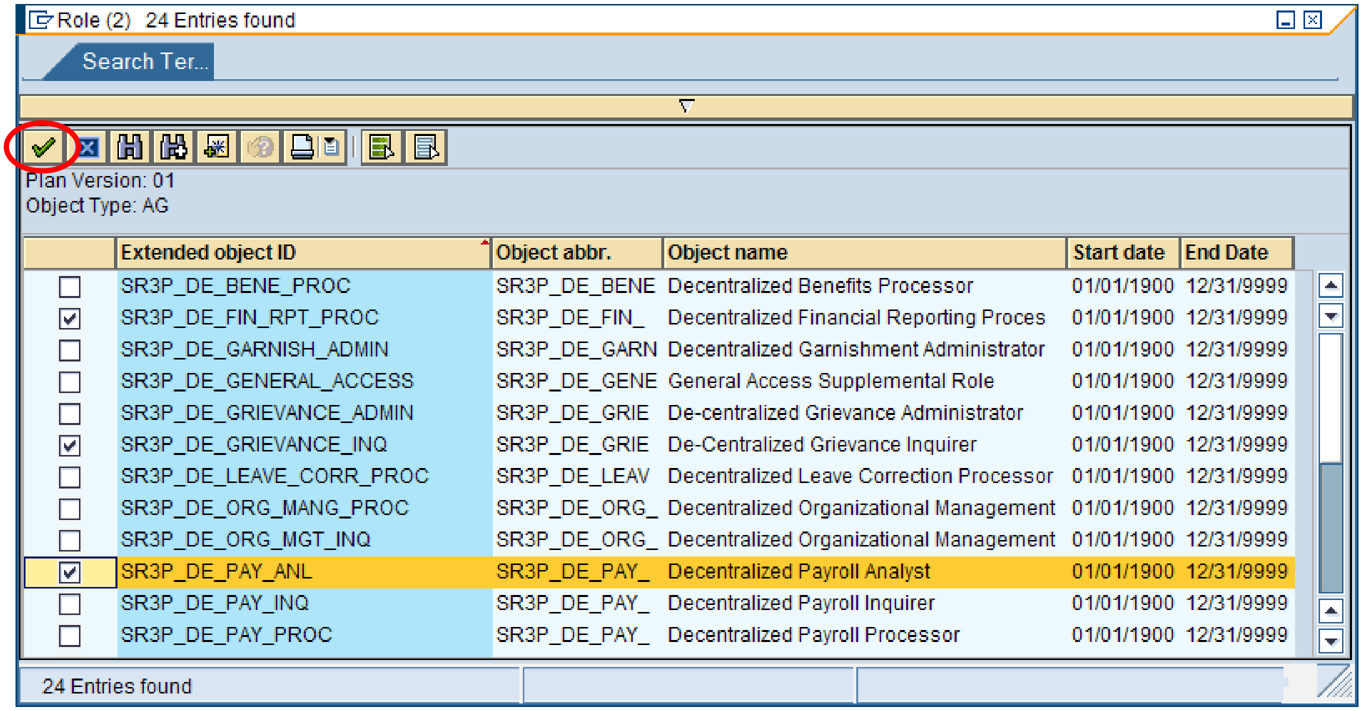


10. Enter SR3P_* to get a list of *all* the roles you can assign.

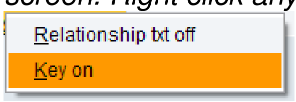


11. In the screen that follows, checkmark the roles that you want to assign to this position.

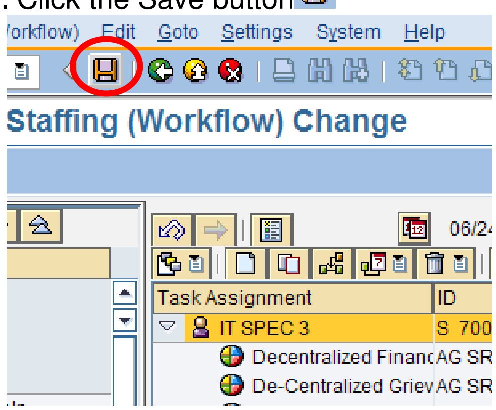
12. Click the Check mark button 



NOTE: *If you don't see the Extended object ID column, go back to step 8, to the Choose Relationship screen. Right click anywhere on the screen and click on Key on.*



13. Click the Save button

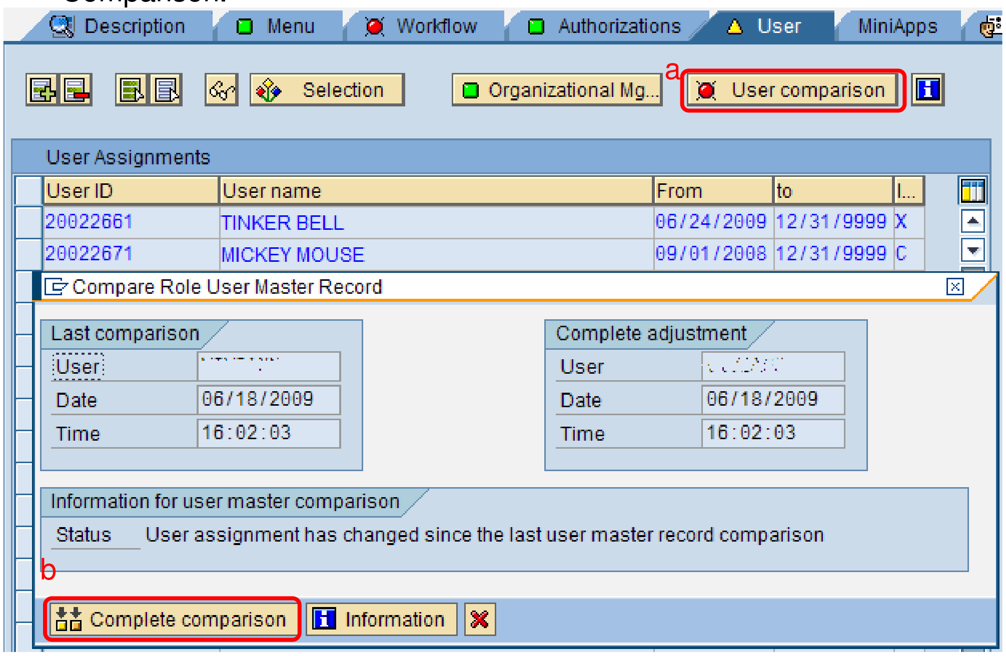


14. To reconcile these newly assigned roles, go to Transaction PFCG, Step 10: Reconciling the Role or complete the next steps.

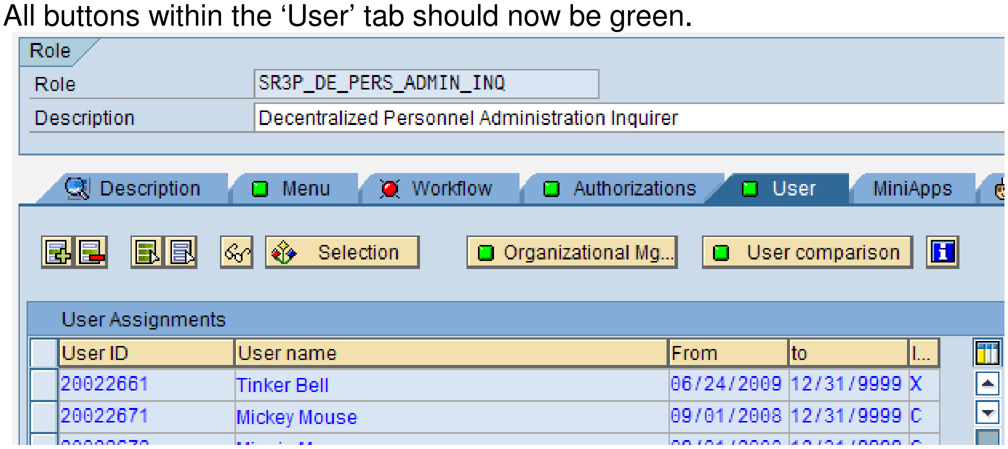
Reconcile the Roles Using SU01D

1. Enter transaction SU01D (/nSU01D)
2. Enter the UserID (8 digit Personnel Number, ***including*** leading zeroes) into the 'User' field, of the employee you just added roles to.
3. Click on to Display.
4. Click on the Roles tab
5. Double click on the red circle to the left of the newly assigned role.
6. Display roles window opens (this is the PFCG screen)
7. Click on the User tab

8. If the 'User comparison' button is red,
    a. Click on the 'User comparison' button
    b. In the Compare Role User Master Record popup, click on 'Complete Comparison.'



9. All buttons within the 'User' tab should now be green.



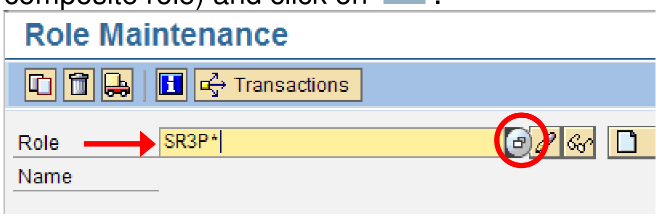
10. Click the 'Save' button to save changes to the role.
11. Close the Change Roles screen
12. Repeat from step 4 to reconcile any additional roles.
13. Contact your User Administrator after all roles are assigned, they need to go to SU01 and complete the steps for maintaining a professional user.

Delete Roles from Positions Using PFCG

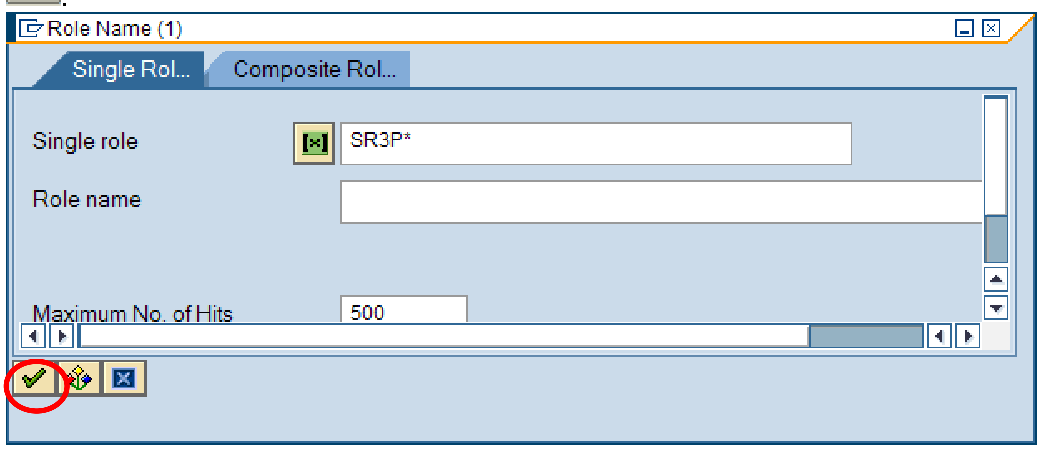
Prerequisites:
✓ Role name(s)
✓ SAP position number(s).

1. Enter transaction '**PFCG**' (/nPFCG) to delete role(s) from position(s).

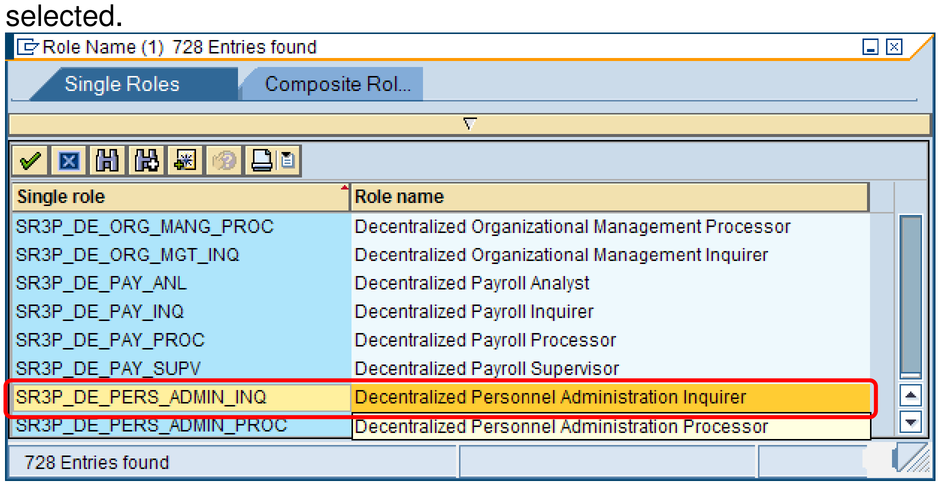
2. If you know the full role name, enter it in the 'Role' field, and skip to Step 5. Otherwise, search for the role that needs to be deleted from the position. Type SR3P* (for single role) or CR3P* (for composite role) and click on .



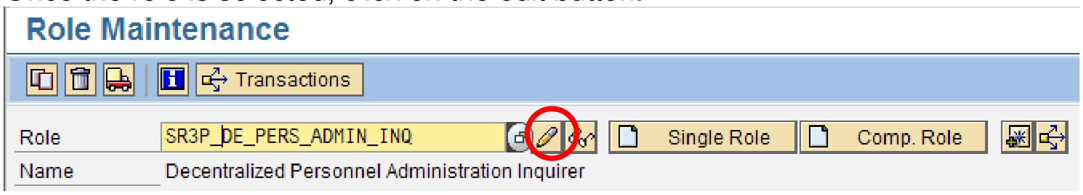
3. Verify/confirm the proper tab ('Single Roles' for SR3P*; 'Composite Roles' for CR3P*) and click on .



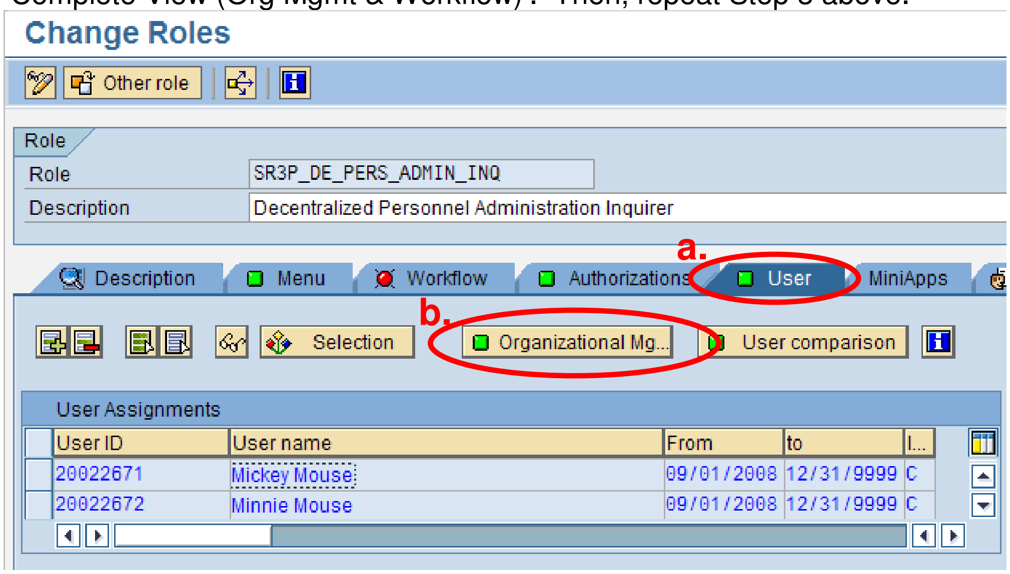
4. Double click on the appropriate role: for this example, 'Personnel Administration Inquirer is selected.



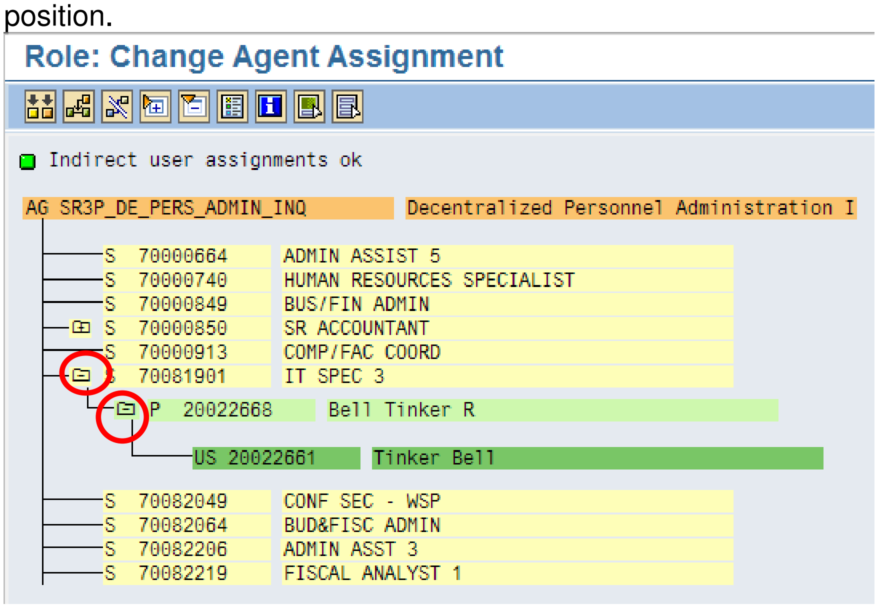
5. Once the role is selected, click on the edit button.



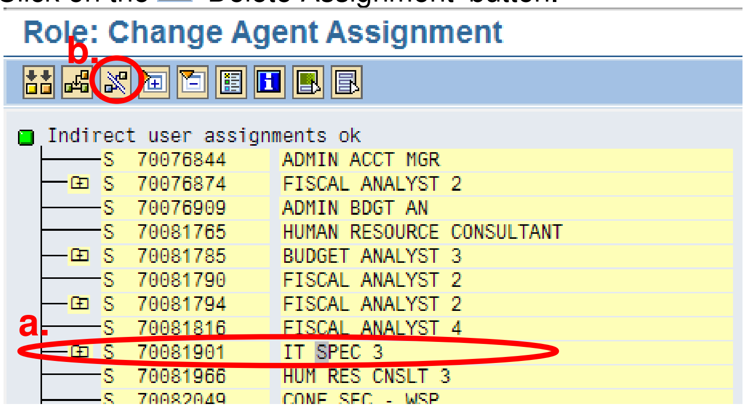
6. Update the Role
   a. Click on the ‘User’ tab
   b. Click on the “Organizational Mg…” button. **IF this button does not appear**, click on the ‘back’ button, then click ‘Goto’ pull-down menu (on menu bar), select ‘Settings” and select ‘Complete View (Org Mgmt & Workflow)’. Then, repeat Step 3 above.



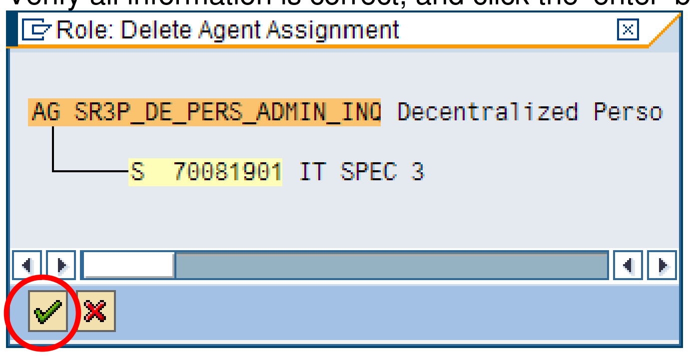
7. To display SAP position numbers, click on ‘View’ on the pull-down menu bar, and then click on ‘Key On’. Click on the to drill down; confirm/verify this change will only impact the correct person and the UserID. If position is “multi-filled”, this action will remove access for all employees in this position.



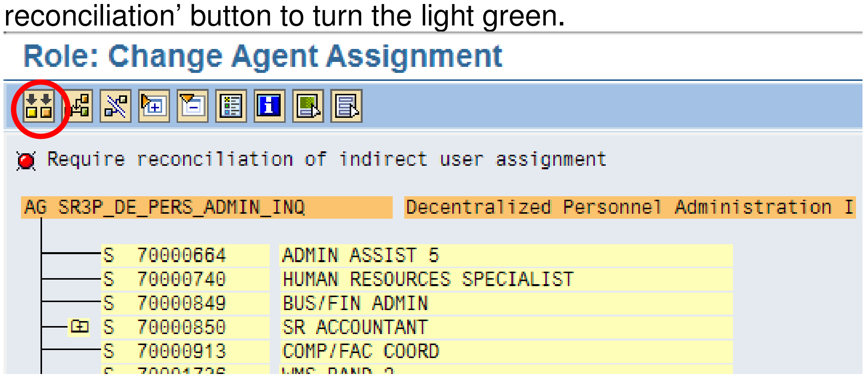
8. Delete the assignment.
   a. Click on the position name (in yellow) to highlight it.
   b. Click on the ‘Delete Assignment’ button.



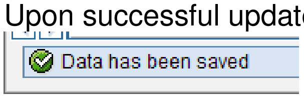
9. Verify all information is correct, and click the ‘enter’ button.



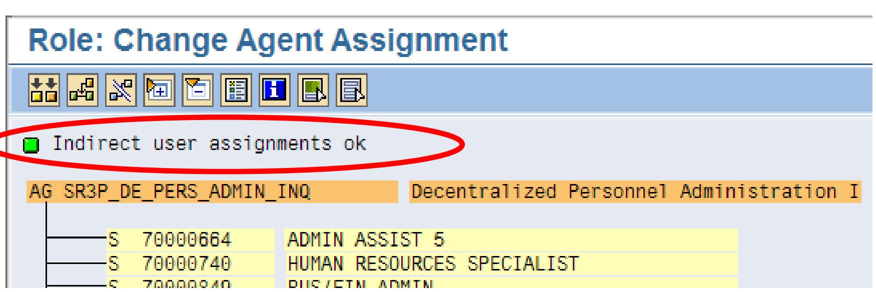
10. Notice the red light and message at the top of the screen; click on the ‘indirect user assignment reconciliation’ button to turn the light green.



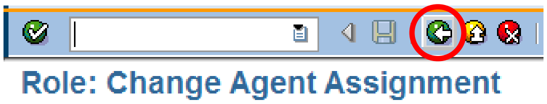
Upon successful update, you will see that the light has turned green, and the message



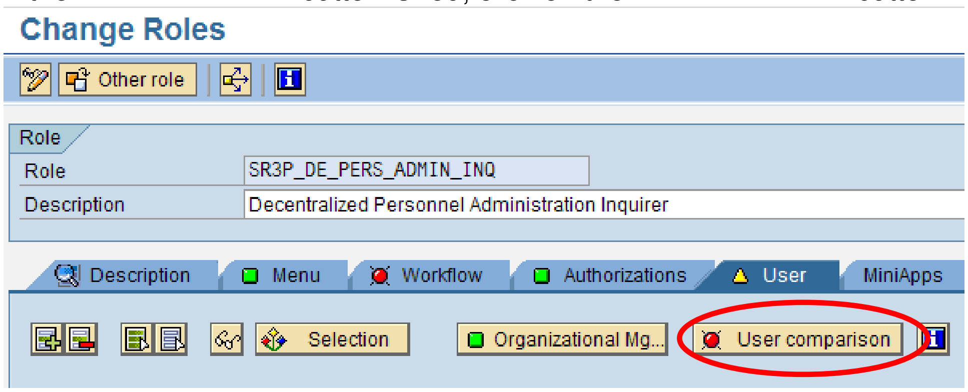
in the status area.



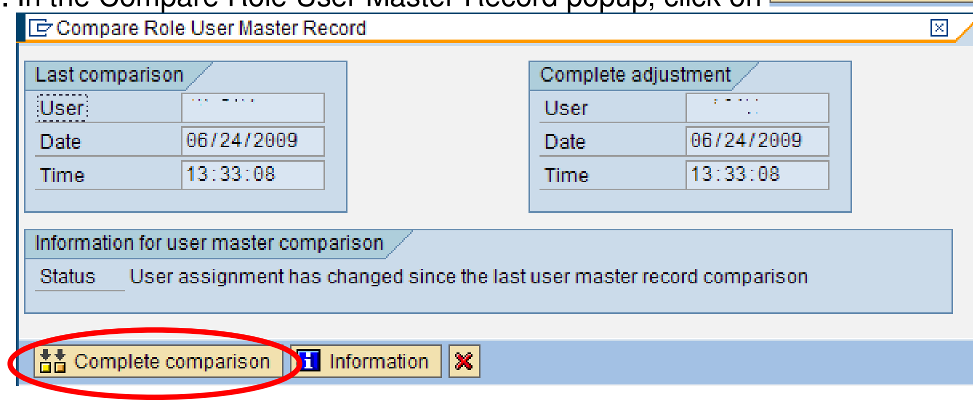
11. Back out of this screen



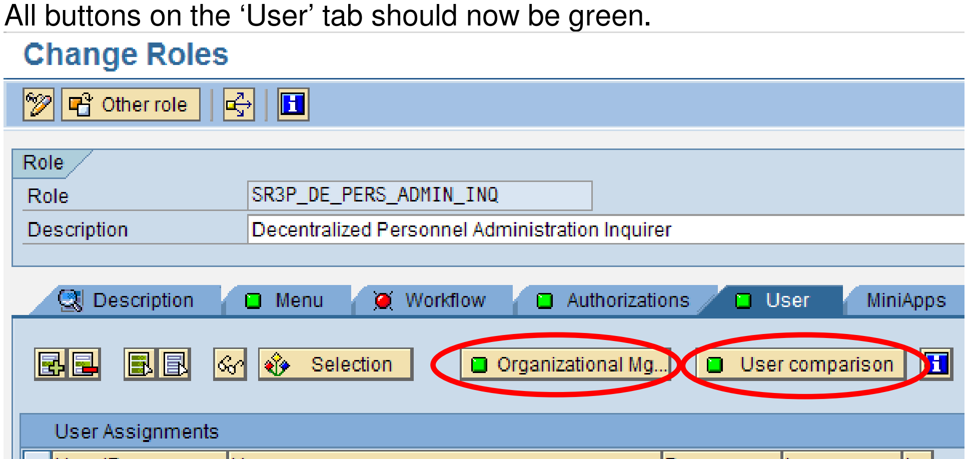
12. If the User comparison button is red, click on the User comparison button.



13. In the Compare Role User Master Record popup, click on Complete comparison



14. All buttons on the 'User' tab should now be green.



15. Click to save your changes. You will see the message Data was saved in the status area.

16. Follow the same steps for Delete Roles from Positions (PFCG) to delete any other roles.

17. If the person is no longer going to be a professional user, contact your User Administrator, they need to go to SU01 and complete the steps for transferring a professional user back to ESS user.

HCM User Administrator SR3P_XXXX_USER_ADMIN

Maintaining a Professional HCM UserID Account

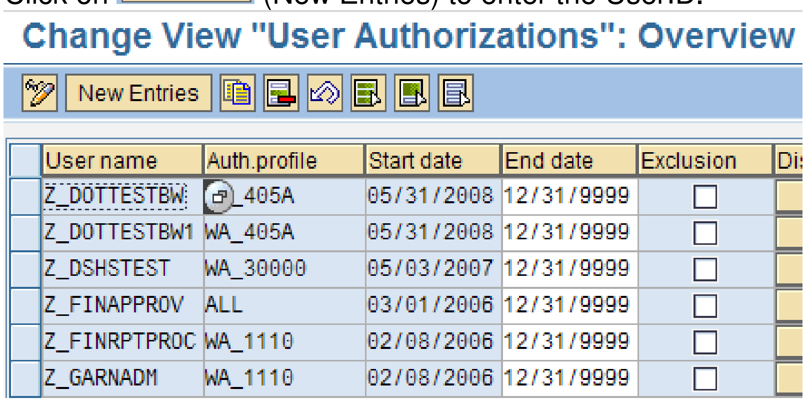
Agency User Administrators will use this process when changing a non-professional (ESSUSER) UserID account to a professional (WA_XXXX) UserID account in order to access HCM.

Prerequisites:

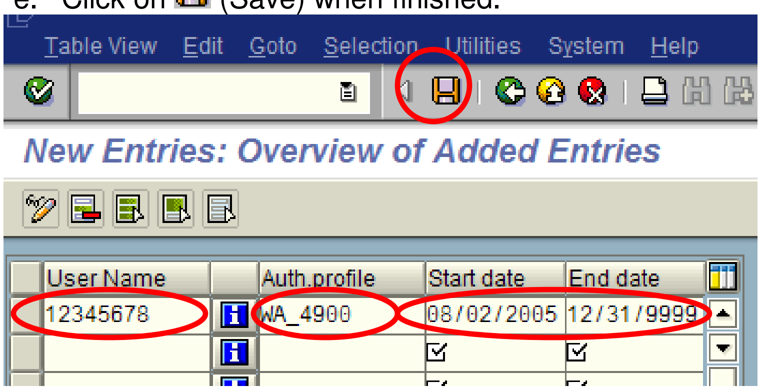
✓ *Professional roles must be assigned to the employee's position by the agency Auth Administrator.*

Enter OOSB Auth Profile

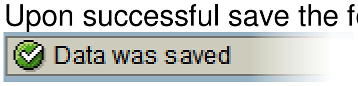
1. Enter transaction '**OOSB**' (/nOOSB) to update table T77UA.
2. Click on New Entries (New Entries) to enter the UserID.



3. Enter the following:
   a. User Name – the UserID (Personnel number, ***including*** leading zeros)
   b. Auth. Profile – The User Group authorization profile (like: WA_4900);
      * Note **Pers Admin Processors require a 2nd entry w/Auth profile 'WA_SOW'.**
   c. Start Date
   d. End Date – if an exact date is known it should be entered, otherwise use 12/31/9999
   e. Click on (Save) when finished.

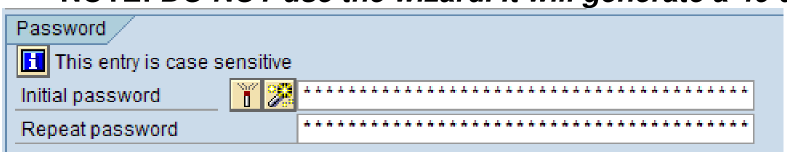


4. Upon successful save the following message will appear

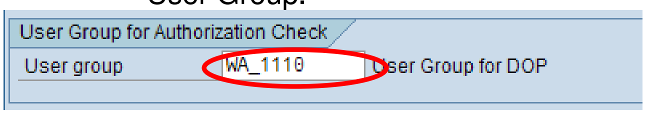


Update the UserID (SU01)

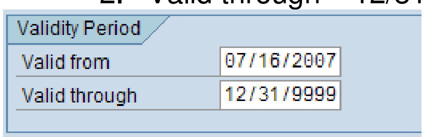
1. Enter transaction SU01
2. Enter the UserID (8 digit personnel number with leading zeros)
3. Click the Display button to verify the user
4. Click on to enter Edit mode
5. From the ‘Logon data’ tab, update the following:
   a. Enter an initial password manually. The password must follow the hardened guidelines (8 characters which contain at least 1 digit, and 1 special character.)
   NOTE: *DO NOT use the wizard. It will generate a 40 digit password.*



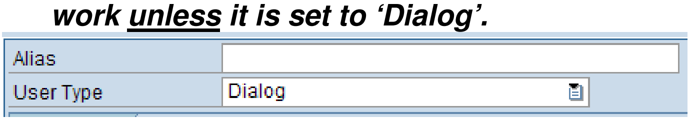
   b. Enter the User Group for your Agency. To search, click on the button to search for your User Group.



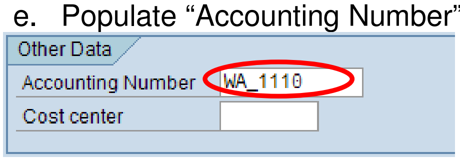
   c. Verify there are Validity Period dates, if there are no dates enter them as follows –
      1. Valid from – date of creation
      2. Valid through – 12/31/9999



   d. Verify that the User Type is set to ‘Dialog’ ***- this is very important, as the UserID will not work <u>unless</u> it is set to ‘Dialog’.***

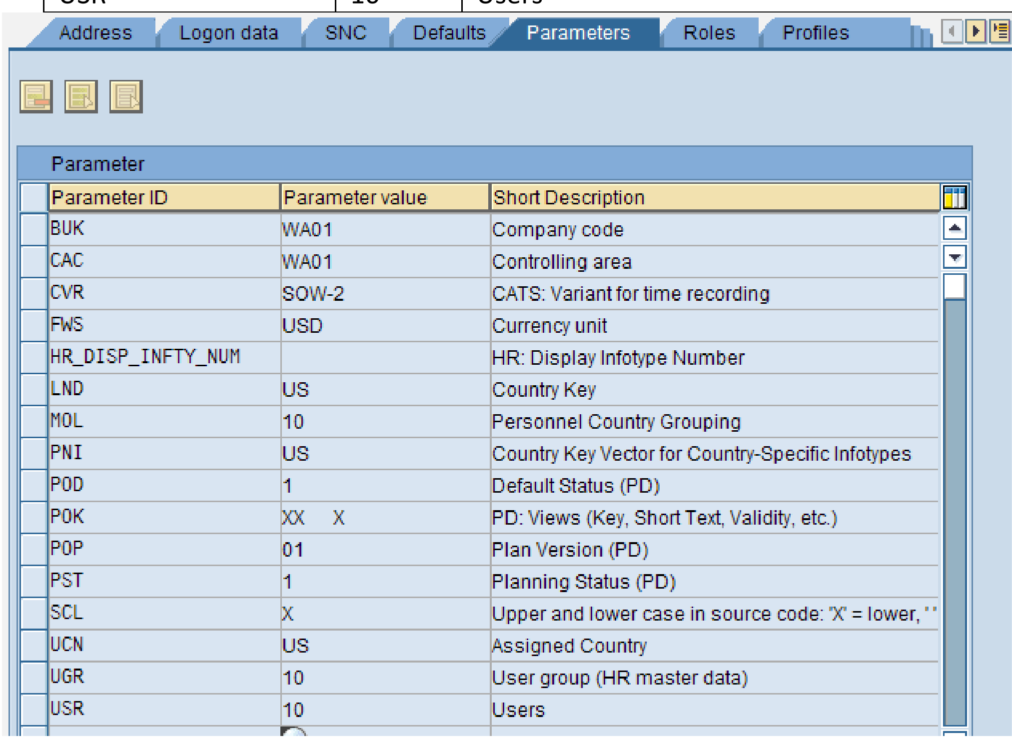


   e. Populate “Accounting Number” field in “Other Data” with User Group data from 9b above

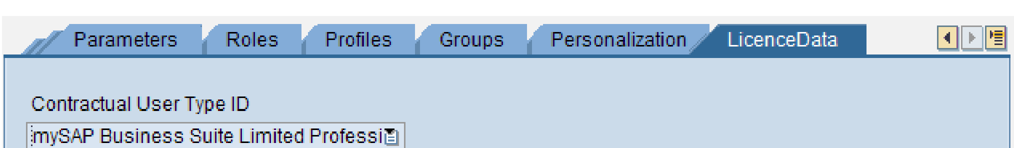


6. Click on the Parameters tab and check the parameters. There should be 16 parameters entered, if the parameters are not entered enter the following parameters:
   NOTE: ***Enter only the Parameter ID and Value and then press enter.***

Parameter ID	Value	Short Description
BUK	WA01	Company code
CAC	WA01	Controlling area
CVR	SOW-2	Variant for time recording
FWS	USD	Currency unit
HR_DISP_INFTY_NUM		HR: Display Infotype Number
LND	US	Country key
MOL	10	Personnel Country Grouping
PNI	US	Country Key Vector for Country-Specific Infotypes
POD	1	Default Status (PD)
POK	XX	PD: Views (Key, Short Text, Validity, etc.)
POP	01	Plan Version (PD)
PST	1	Planning Status (PD)
SCL	X	Upper and lower case in source code: 'X' = lower, ' ' =upper
UCN	US	Assigned Country
UGR	10	User group (HR master data)
USR	10	Users



Parameter ID	Parameter value	Short Description
BUK	WA01	Company code
CAC	WA01	Controlling area
CVR	SOW-2	CATS: Variant for time recording
FWS	USD	Currency unit
HR_DISP_INFTY_NUM		HR: Display Infotype Number
LND	US	Country Key
MOL	10	Personnel Country Grouping
PNI	US	Country Key Vector for Country-Specific Infotypes
POD	1	Default Status (PD)
POK	XX X	PD: Views (Key, Short Text, Validity, etc.)
POP	01	Plan Version (PD)
PST	1	Planning Status (PD)
SCL	X	Upper and lower case in source code: 'X' = lower, ' '
UCN	US	Assigned Country
UGR	10	User group (HR master data)
USR	10	Users

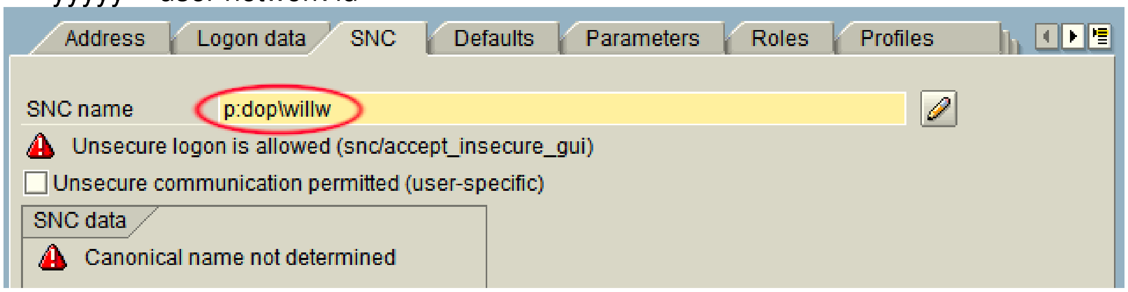


7. Save the account

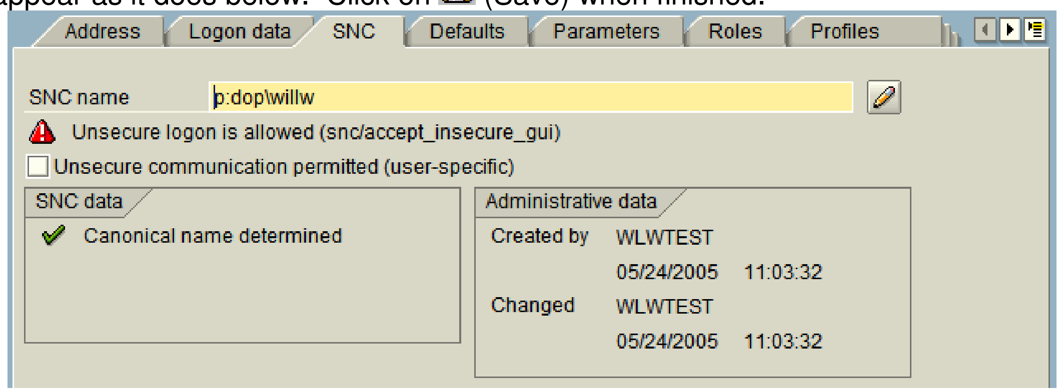
If NOT using Single Sign On (SSO) you are done. If you ARE using SSO continue to step 14.

Single Sign On (SSO)

8. Click the "SNC' tab. Enter the SNC name in the following format 'p:xxx\yyyy' (see example below).
   - xxx = 3 letter agency code
   - yyyyy = user network id



9. If the update is successful, a green check mark and the message "Canonical name determined" will appear as it does below. Click on (Save) when finished.



HCM UserID Maintenance

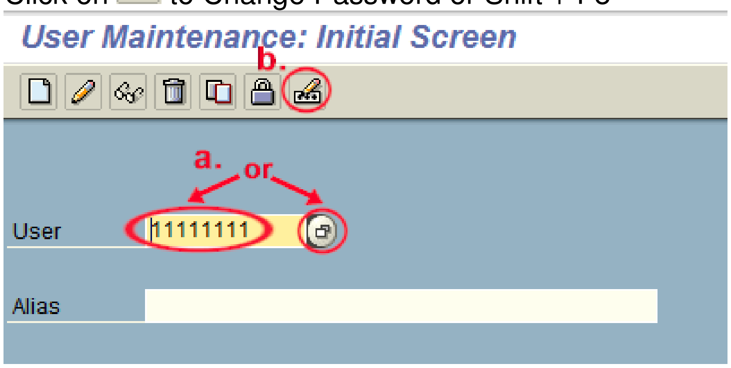
Reset HCM Password (SU01)

1. Enter transaction '**SU01**' (/nSU01) to reset the password

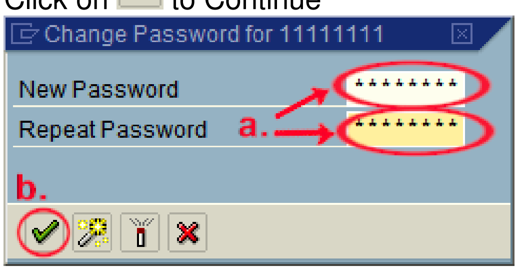
2. Enter the UserID for which you are re-setting the password.
   a. Enter the UserID (8 digit Personnel Number, ***including*** leading zeroes) into the 'User' field. In this example it is '11111111'. To search for the User, click on  to search and select the User.

NOTE: *Users will not be unlocked by resetting the password so always check if the user is locked by clicking on the*  *Lock button. Unlock the user if needed.*

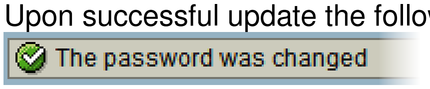
   b. Click on  to Change Password or Shift + F8



3. Enter the new password **Manually**
   a. Enter the new password and repeat for verification (Hardened password standards apply; passwords must contain at least one letter, one number, one special character and be at least eight characters long)
   b. Click on  to Continue



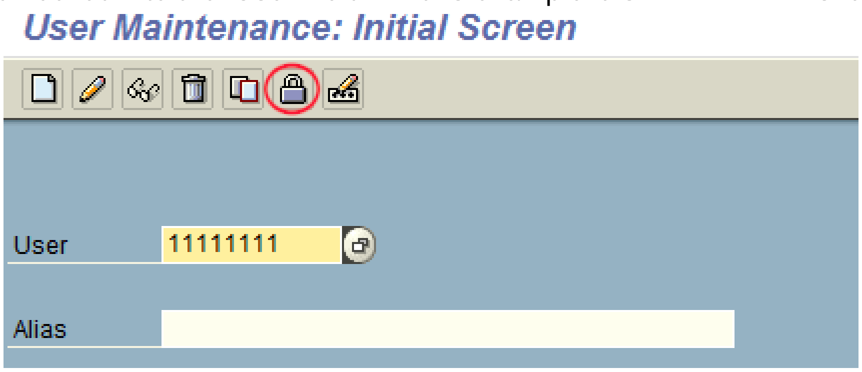
4. Upon successful update the following message will be displayed. Notify User of new password.



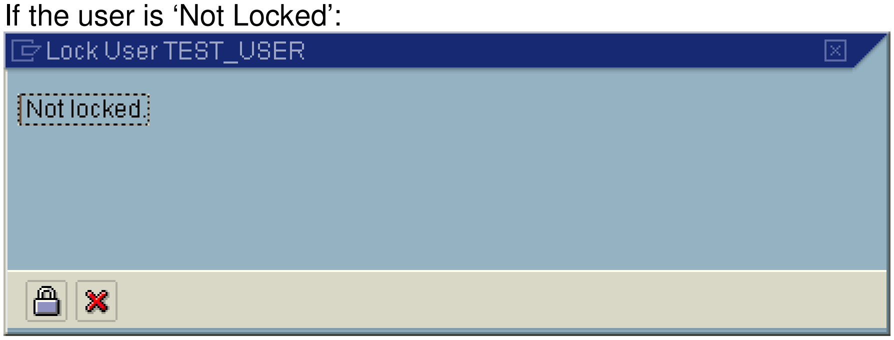
Lock/Unlock HCM UserID (SU01)

1. Enter transaction ‘**SU01**’ (/nSU01) to lock or unlock a UserID

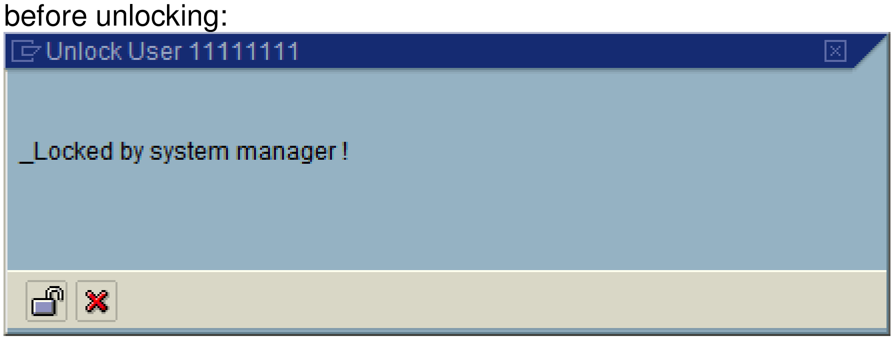
2. Enter the UserID (8 digit Personnel Number, ***including*** leading zeroes) that needs to be locked or unlocked into the ‘User’ field. In this example it is ‘11111111’. Click the ‘Lock/Unlock’ button.



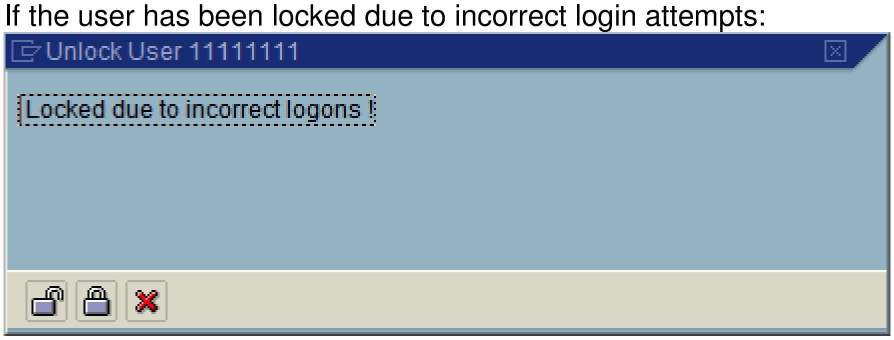
3. A screen indicating the Lock Status of the User will appear.
   a. If the user is ‘Not Locked’:



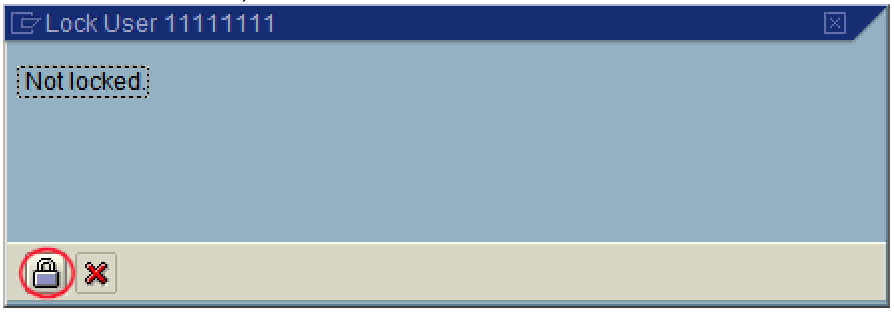
   b. If the user has been locked by the System Manager, there may be a specific reason, research before unlocking:



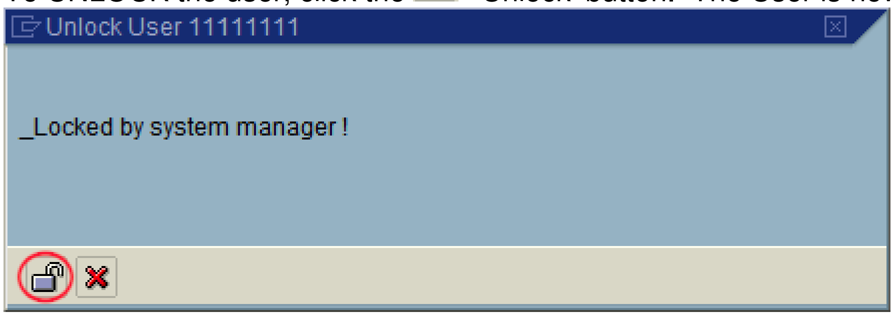
   c. If the user has been locked due to incorrect login attempts:



4. To LOCK the user, click the 'Lock' button. The User is now locked.



5. To UNLOCK the user, click the 'Unlock' button. The User is now unlocked.

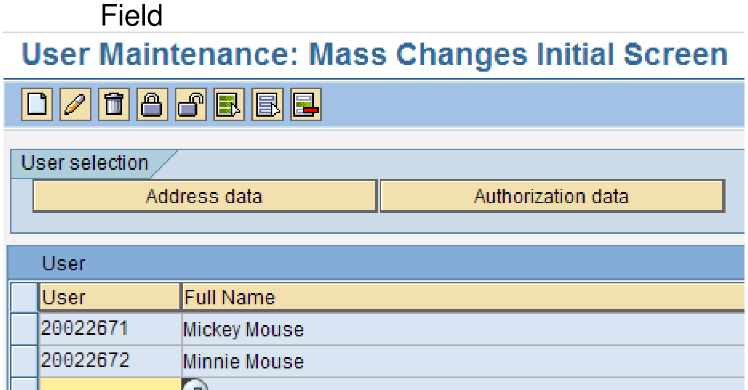


Mass HCM UserID Lock/Unlock (SU10)

There are many options for Mass User Maintenance, including locking of UserIDs, changing Parameters and/or Defaults, etc.

1. Enter transaction '**SU10**' (/nSU10) to lock or unlock multiple UserIDs

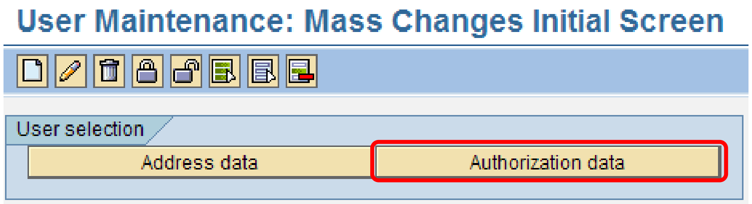
2. Select the Users to be Unlocked.
   Option 1 – Enter the users manually
   a. Enter the UserIDs (8 digit personnel number ***including*** leading zeroes) manually into the User Field



   b. Click the Lock or Unlock button, depending on whether you need to lock or unlock the users.

Option 2 – Select Users from a list

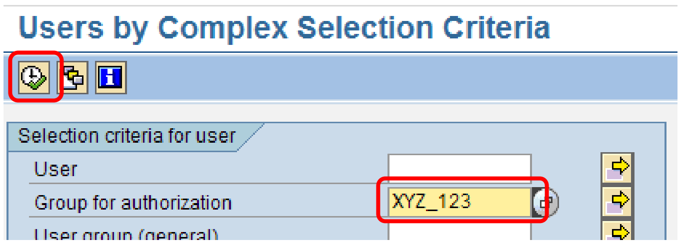
a. Click on the Authorization data button



b. Search on the User Group (like WA_1110). You can also search using any of the other options to refine the results.

c. Enter the '*Group for Authorization*', in this example it is XYZ_123. This would be your specific Agency's User Group.

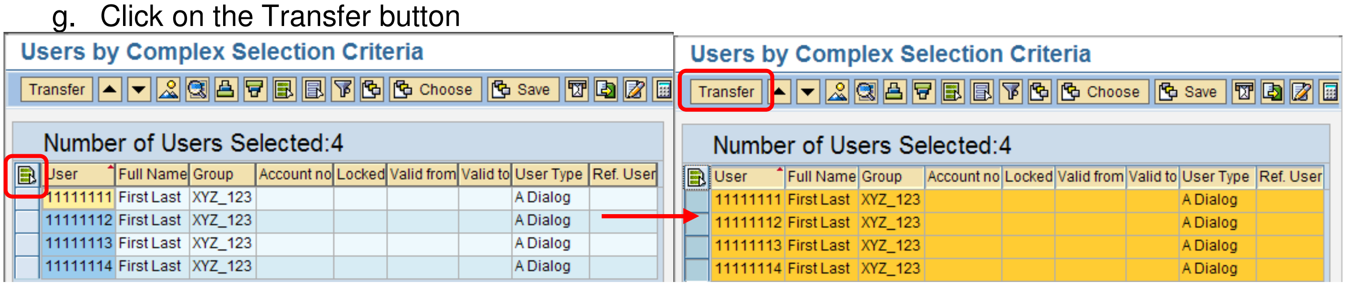
d. Click on [execute icon] to execute the search.



e. Select and Transfer the Users to update

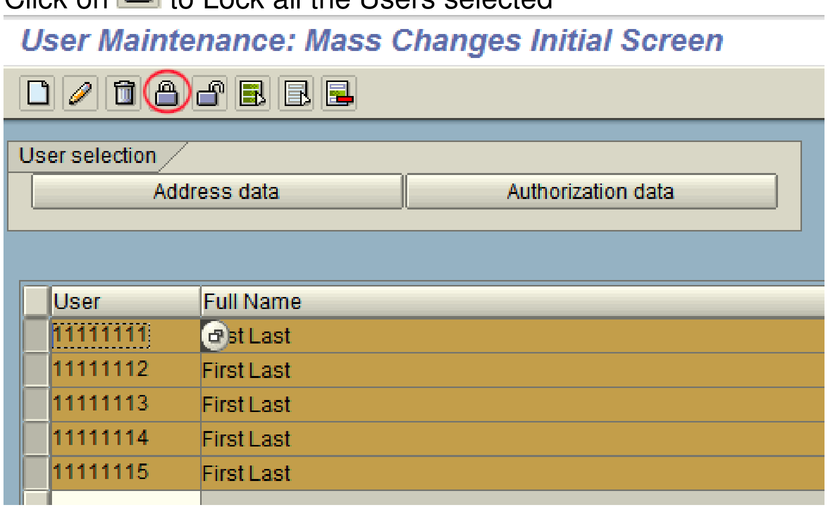
f. Click on the [Select All icon] (Select All button) or select individual users

g. Click on the Transfer button

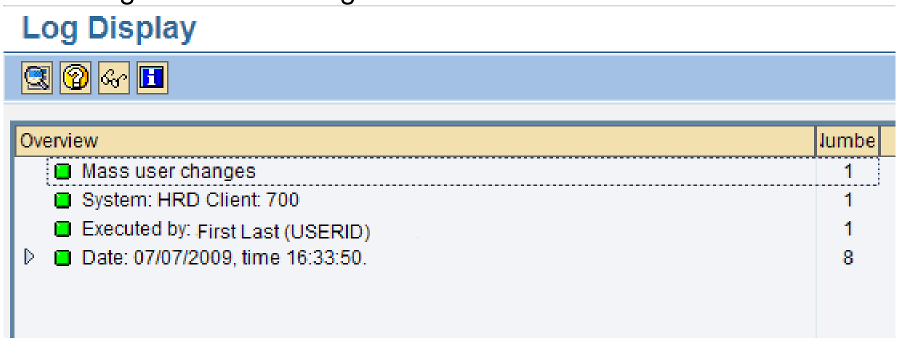


h. To LOCK Selected Users

1. Click on [lock icon] to Lock all the Users selected

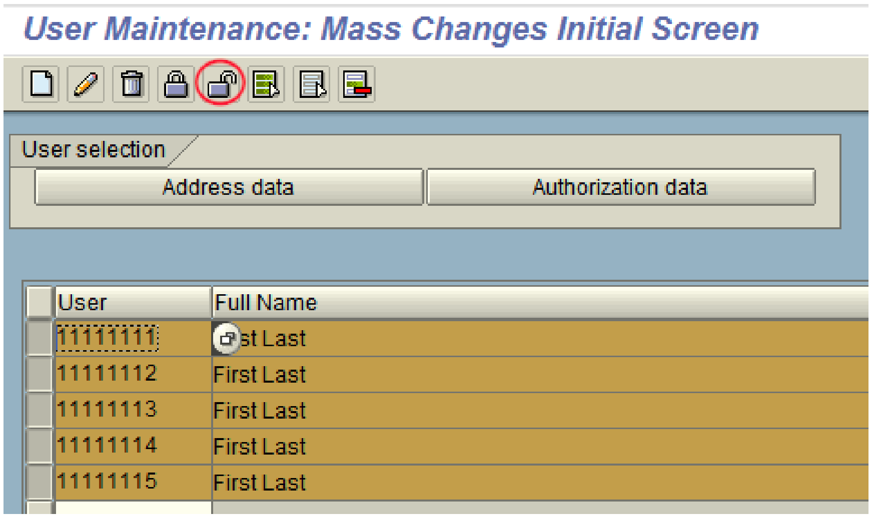


2. A log screen similar to the one below will appear. Click on the Expand button ; the expanded view will give a detailed log of each user that was locked

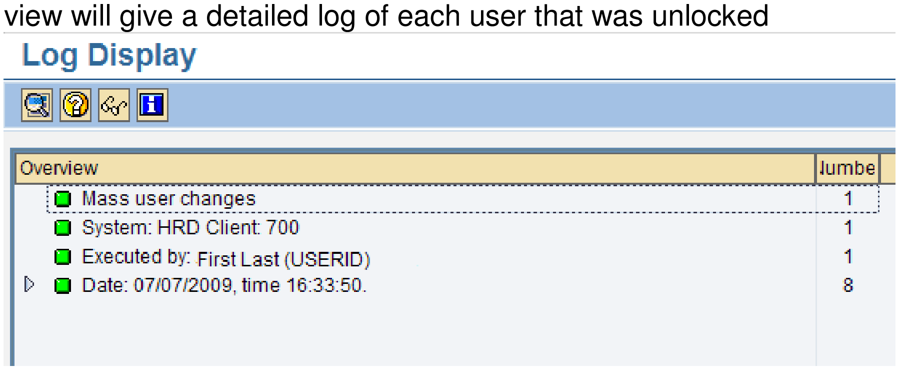


i. To UNLOCK Selected Users

1. Click on to Unlock all the Users selected



2. A log screen similar to the one below will appear. Click on the Expand button ; the expanded view will give a detailed log of each user that was unlocked



Non-Professional Users (ESS Users) Leave State Employment – Employee Status is Withdrawn:

NOTE: *DOP recommends to keep the SU01 UserID account for withdrawn employees for at least 30 days after the termination of state employment. This account gives the user the authorizations to see their earnings statement in the Portal.*

HCM:

1. Login to HCM – HRMS Production (RP0) – through the SAP Logon Pad
2. Verify the employee is withdrawn
   1. Enter transaction PA20
   2. Enter employee's personnel number
   3. Click the Overview button
   4. Check the Status: Withdrawn

Name	[illegible]						
PersArea	4650	Parks/Recreation Comm		EEGroup	H	Non-Perm. Limited	
PSubarea	0001	Non Represented	EESubgroup	05	H-OT Elig>40hrs/wk	Status	Withdrawn

3. Enter transaction '**SU01**' (/nSU01)
4. Enter the UserID (Personnel Number, ***including*** leading zeroes) into the 'User' field.
5. Click the Display button to verify the user
6. Click on the Back button to go back to the User Maintenance screen
7. Click the Delete button and delete the account.

NOTE: *Portal User Administrator needs to delete personnel number UserID from the Portal.*

Professional Users Transfer out of the Agency or Professional Users Become Non-Professional Users (ESS Users):

HCM:

1. Login to HCM – HRMS Production (RP0) – through the SAP Logon Pad

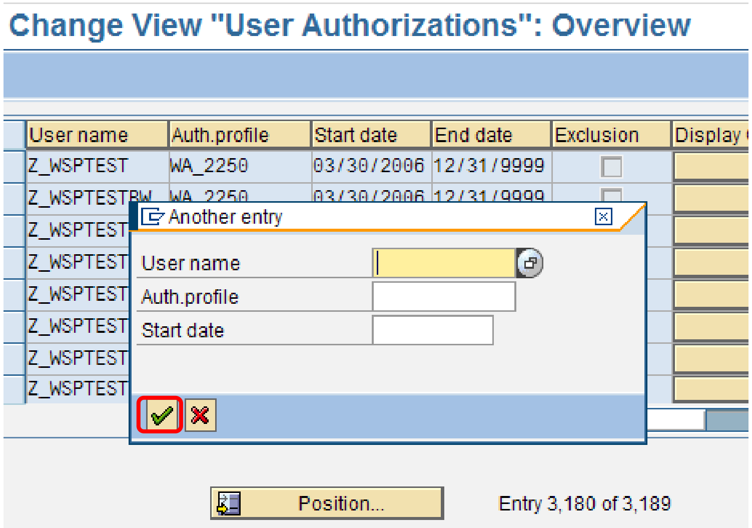
If the employee's employment status is **active or inactive (PA20)**, and no longer in your agency

2. Verify the employee status is active/inactive
   1. Enter transaction PA20
   2. Enter employee's personnel number
   3. Click the Overview button
   4. Check the Status: Active or Inactive

Name	[illegible]						
PersArea	1000	Attorney General		EEGroup	B	Civil Service Exempt	
PSubarea	0001	Non Represented	EESubgroup	01	Monthly(M) OT Exem...	Status	Active

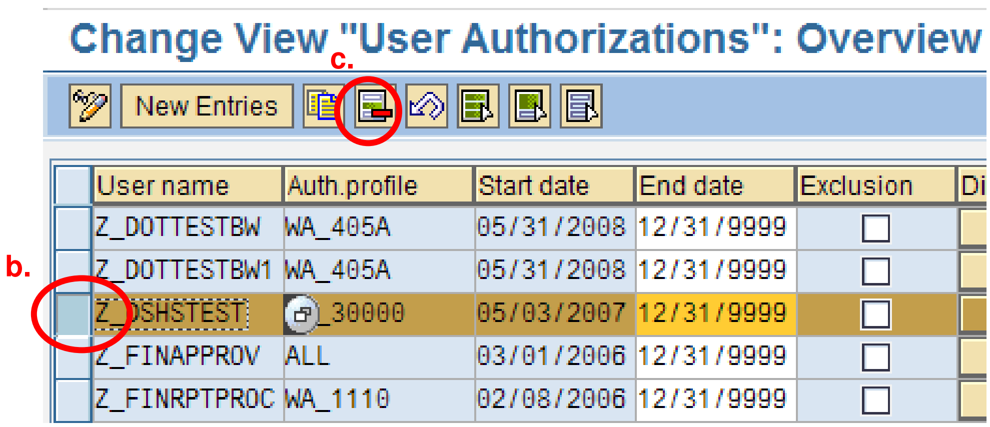
Name	[illegible]						
PersArea	2450	Military Department		EEGroup	0	Permanent	
PSubarea	0001	Non Represented	EESubgroup	01	Monthly(M) OT Exem...	Status	Inactive

3. Enter transaction '**OOSB**' to remove the authorization (/nOOSB).
   a. Click the "Position" button at the bottom of the screen and enter the eight digit UserID in the User name field and click the green check mark. That will position the list to the selected UserID



b. Click the box to the left of the UserID

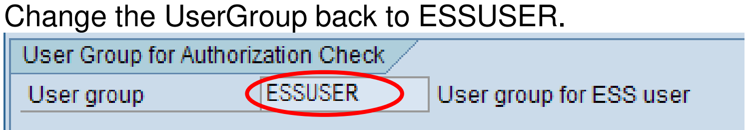
c. Click to delete the entry. Repeat for all entries for this UserID that are associated with the user's access in **your** agency/personnel area.



You will see  in the status area.

d. Click the Save button to save the table.

4. Enter transaction '**SU01**' (/nSU01) to update the UserID.
5. Enter the UserID (8 digit Personnel Number, ***including*** leading zeroes) into the 'User' field.
6. Click on the Display button , and verify the user.
7. In the Logon Data tab; Click on Display/Change button to enter the edit mode.
8. Change the UserGroup back to ESSUSER.

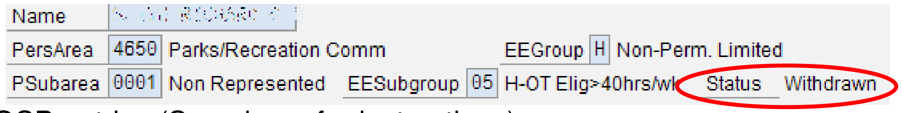


9. Click on Save button to save the account.

If the employee's employment status is **withdrawn (PA20)**

1. Verify the employee is Withdrawn
   a. Enter transaction PA20
   b. Enter employee's personnel number

c. Click the Overview button
d. Check the Status: Withdrawn



2. Remove OOSB entries (See above for instructions)

NOTE: *DOP recommends to keep the SU01 UserID account for withdrawn employees for at least 30 days after the termination of state employment. This account gives the user the authorizations to see their earnings statement in the Portal.*

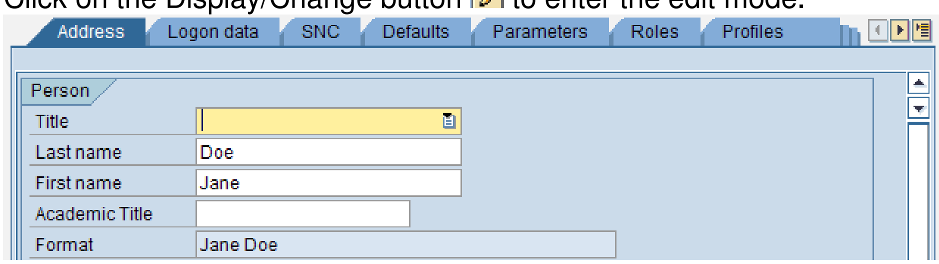
3. Enter transaction '**SU01**' (/nSU01)
4. Enter the UserID (8 digit Personnel Number, ***including*** leading zeroes) into the 'User' field.
5. Click the Display button to verify the user.
6. Click on the Back button to go back to the User Maintenance screen.
7. Click the Delete button and delete the account.

NOTE: *BI and Portal User Administrators need to do clean up on these professional user accounts if the users had access to those systems.*

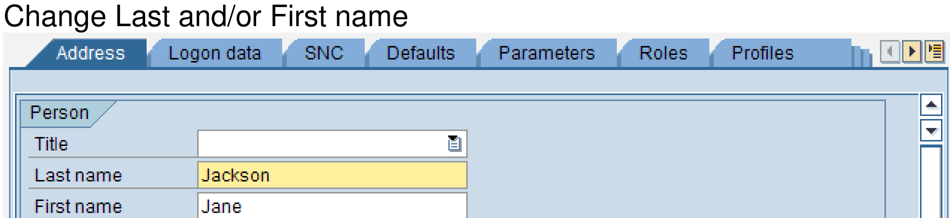
Employee has a Name Change

NOTE: *When an employee has a name change and the HCM personnel master record is updated, this change does not update the UserID account (SU01) for that employee in HCM. The Agency User Administrator must manually go into SU01 and change employee's name.*

1. Enter transaction SU01
2. Enter the UserID (8 digit Personnel Number, ***including*** leading zeroes) into the 'User' field.
3. Click the Display button to verify the user.
4. Click on the Display/Change button to enter the edit mode.



5. Change Last and/or First name



6. Click on Save to save the account.

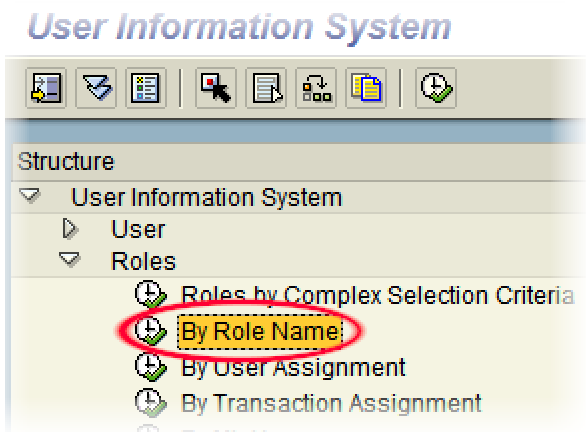
HCM Security Auditor
SR3P_XXXX_SECURITY_AUDIT

Display Users by Role (SUIM)

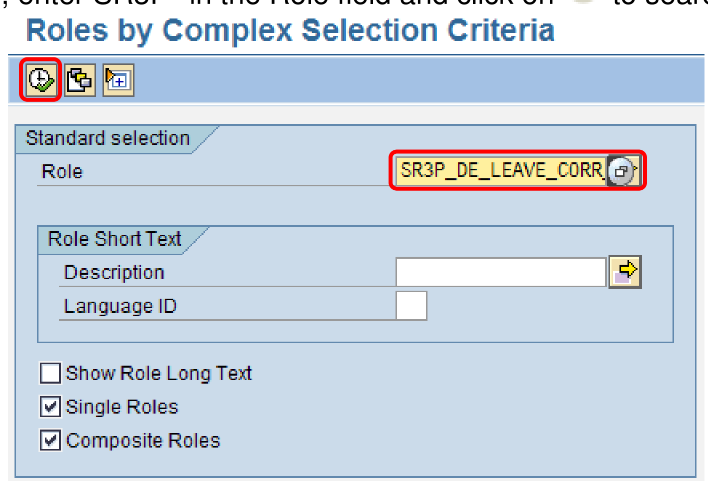
1. Enter transaction '**SUIM**' (/nSUIM) to Display Users by Role

2. Display Users for a Specific Role

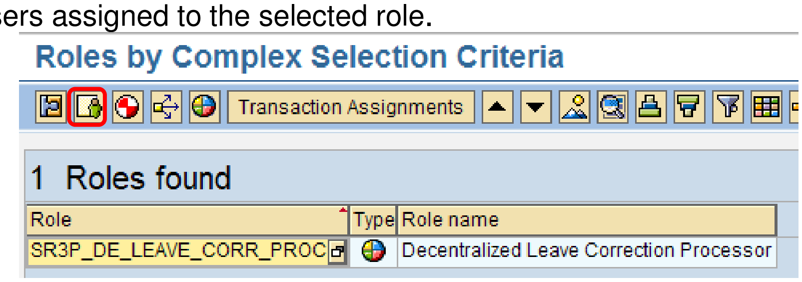
3. From the User Information System screen, drill down to Roles > By Role Name and click on to Execute.



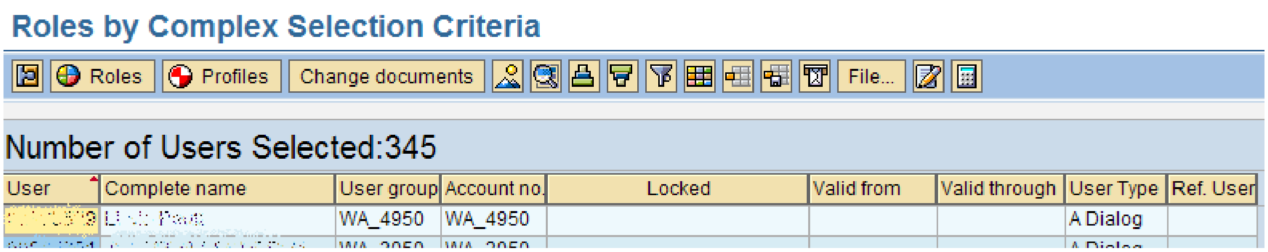
4. Enter the role name (or search if you don't know it) and click on to Execute. To search for the Role, enter SR3P* in the Role field and click on to search.



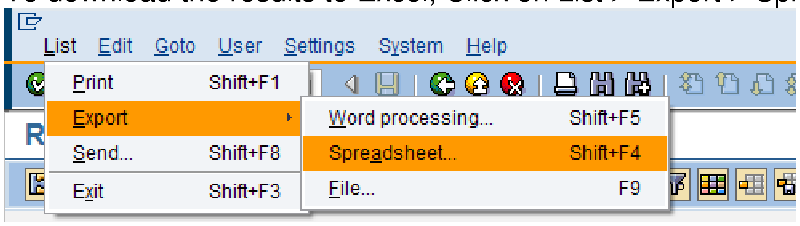
5. From the Roles by Complex Selection Criteria screen, select User Assignment to display all users assigned to the selected role.



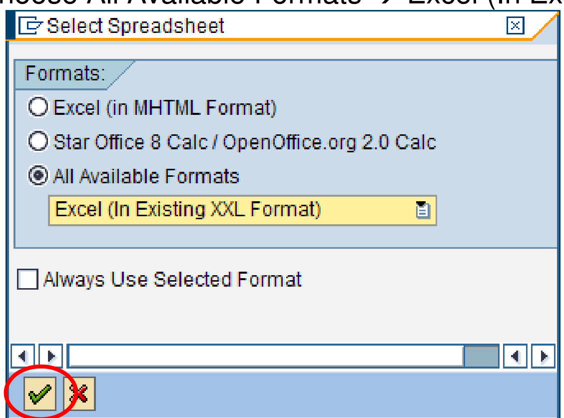
6. A list of Users will be generated.



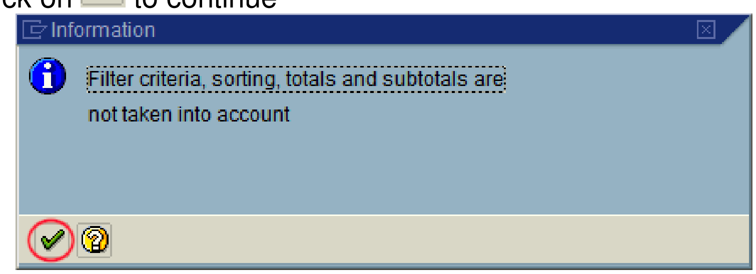
7. To download the results to Excel, Click on List > Export > Spreadsheet



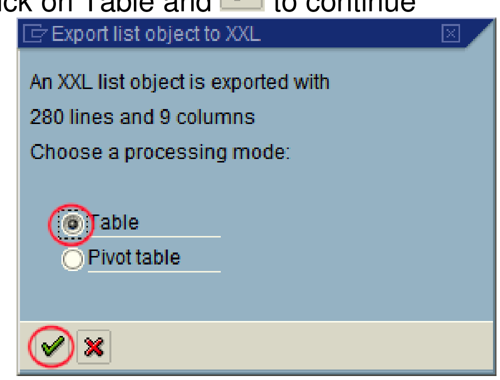
8. Choose All Available Formats → Excel (In Existing XXL Format) and Click on to continue



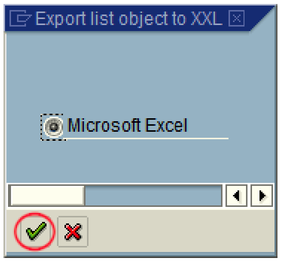
9. Click on to continue



10. Click on Table and to continue



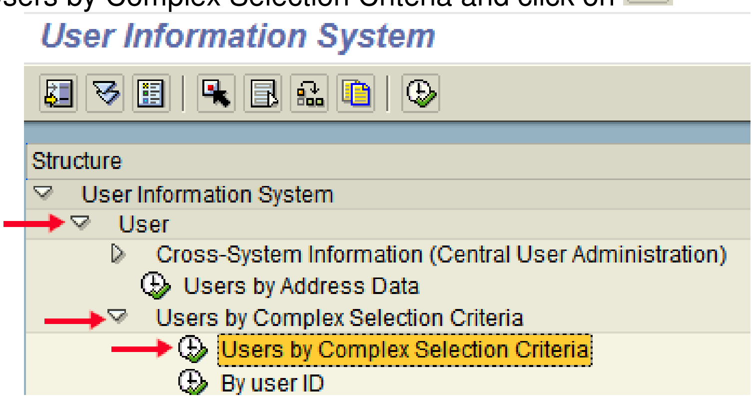
11. Click on  to continue



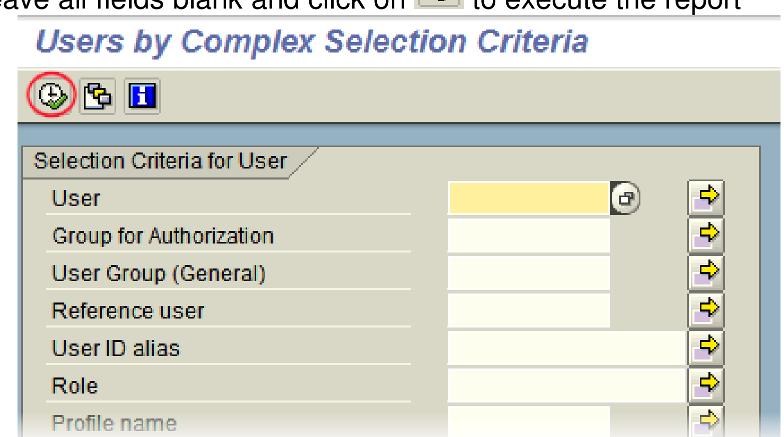
12. Excel will open and display the data.
13. Save the spreadsheet on your computer.

Display Role Assignments for all Users (SUIM)

1. Enter transaction SUIM
2. From the User Information System screen, drill down to User > Users by Complex Selection Criteria > Users by Complex Selection Criteria and click on 

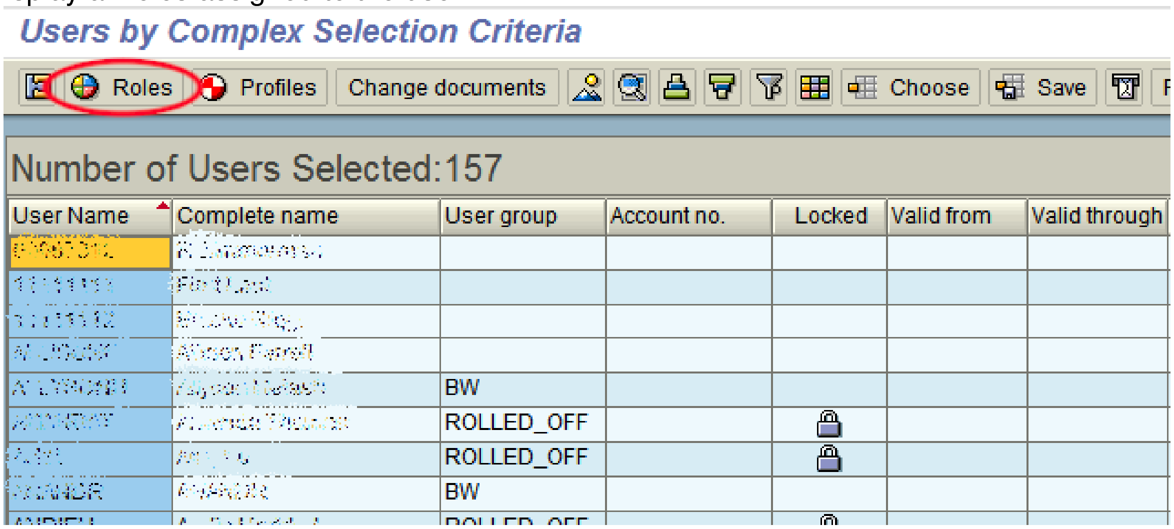


3. Leave all fields blank and click on  to execute the report



4. The list returned should contain all UserID within the agency. Click on the 

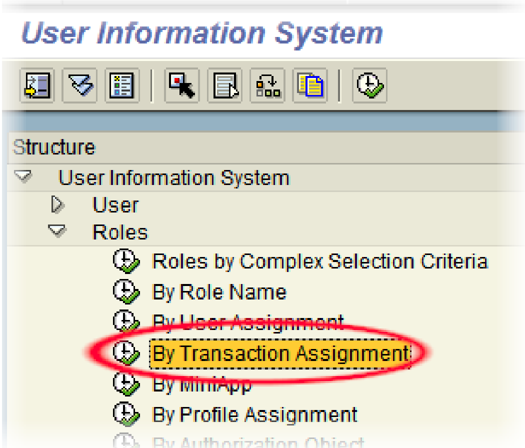
(Roles) button to display all roles assigned to the user.



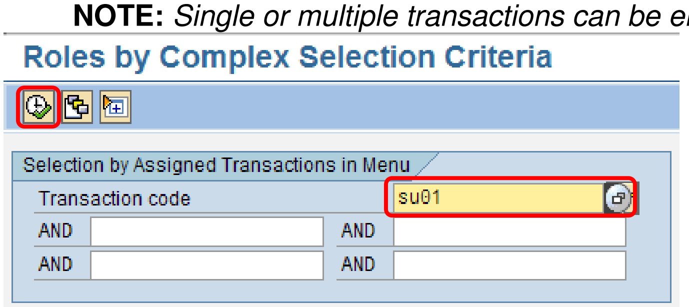
5. The report will be displayed. To download the results to Excel see the steps 7 – 13 in the Display Users by Role above.

Display Transactions by Role (SUIM)

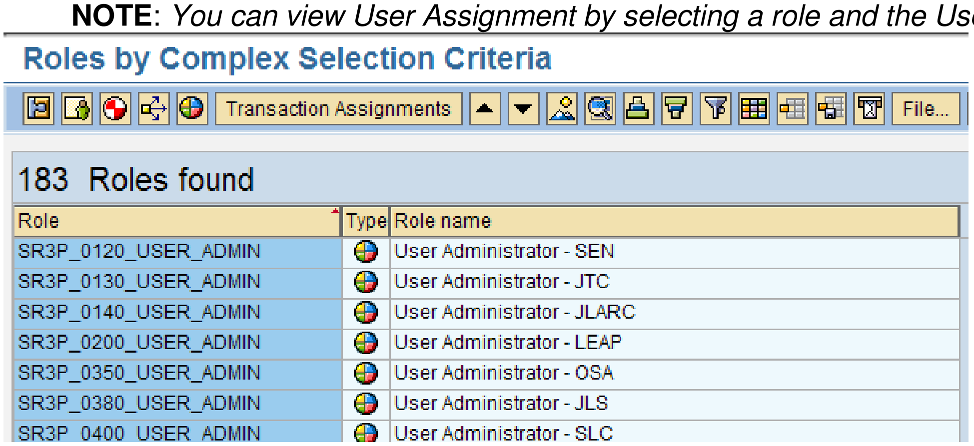
1. Enter transaction '**SUIM**' (/nSUIM) to Display Transactions by Role
2. From the User Information System screen, drill down to Roles > By Transaction Assignment and click on  to Execute.



3. Enter the transaction (or search if you don't know it) and click on  to Execute.
   NOTE: *Single or multiple transactions can be entered here.*



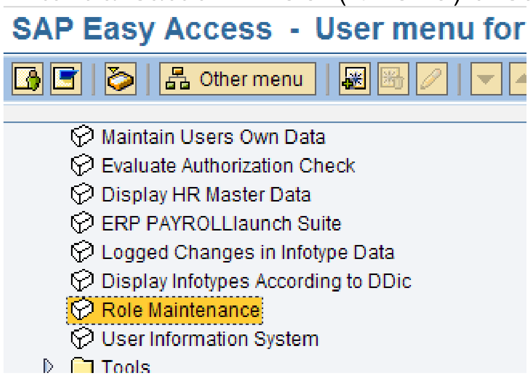
4. A list of Transactions by Roles will be generated.
   NOTE: *You can view User Assignment by selecting a role and the User assignment button.*



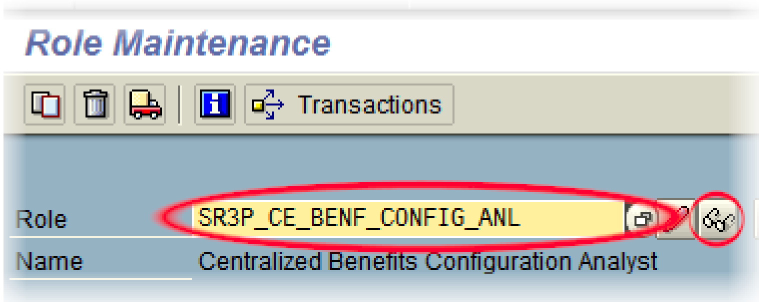
Display Role Information (PFCG)

NOTE: *To see transaction codes in the User Menu click on Extras → Settings, check the Display Technical Names check box and click the green checkmark button.*

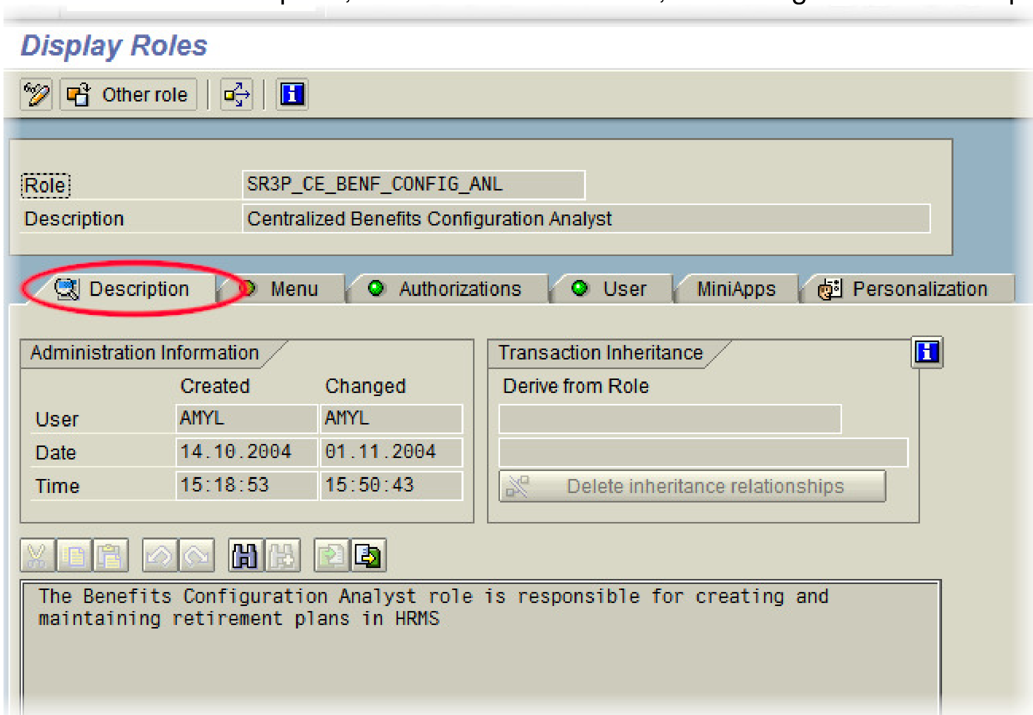
1. Enter transaction '**PFCG**' (n/PCFG) or select 'Role Maintenance' from the main menu.



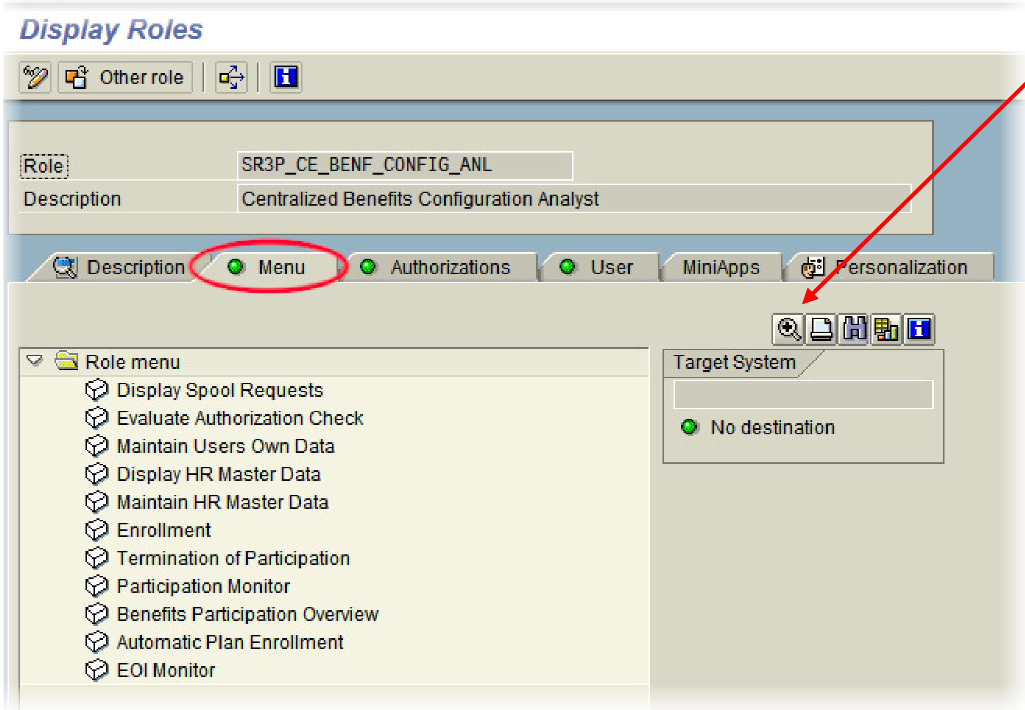
2. Enter the Role Name (or search for possible values) and click on  to Display



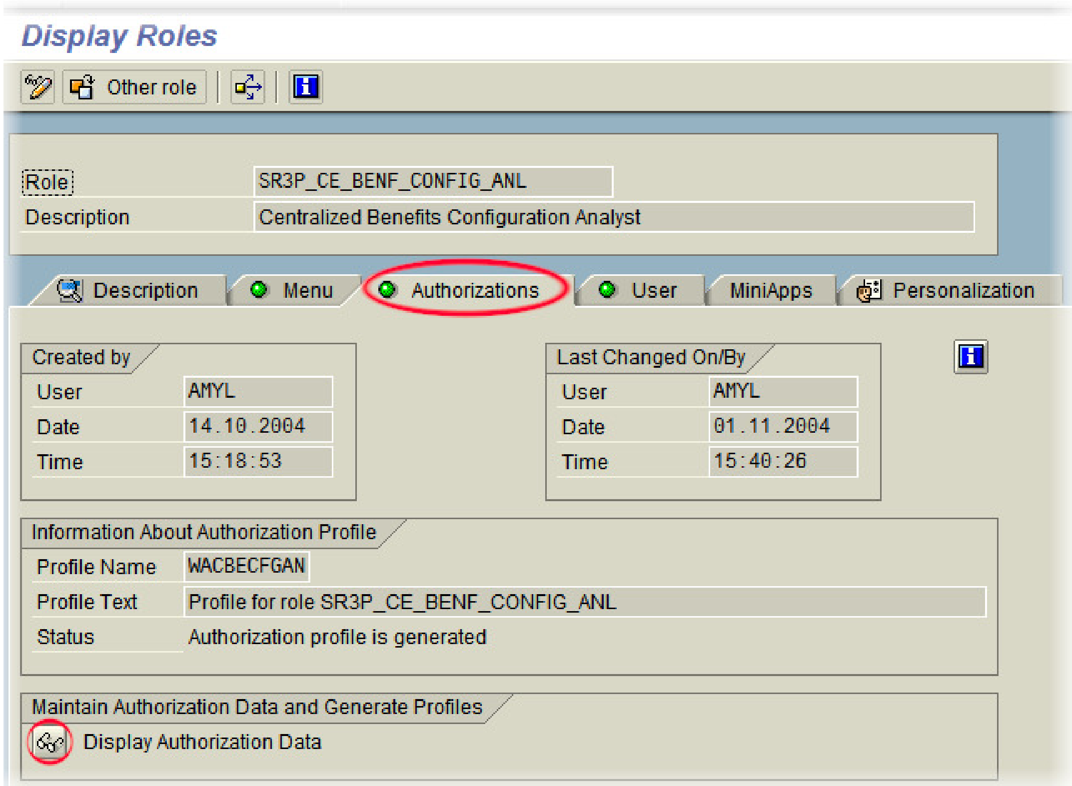
3. The first tab is Description; it will list who created it, last changed and a description.



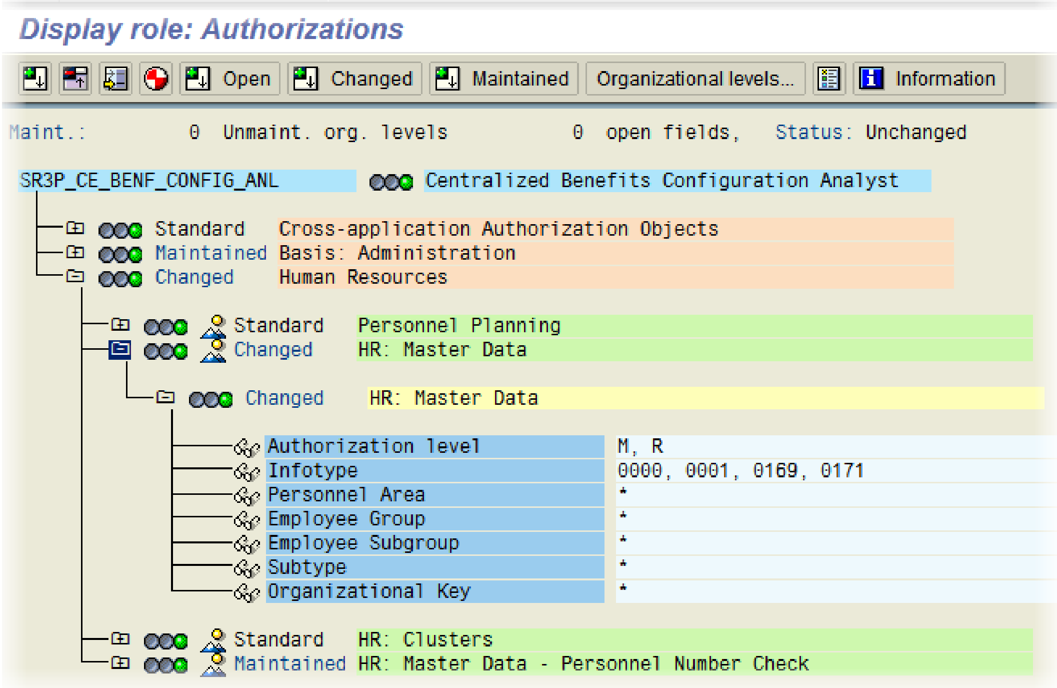
4. The second tab is Menu; this shows transactions available via the menu system for this role.
NOTE: *To see transaction codes in this view click on the 'Switch on technical names'* *button.*



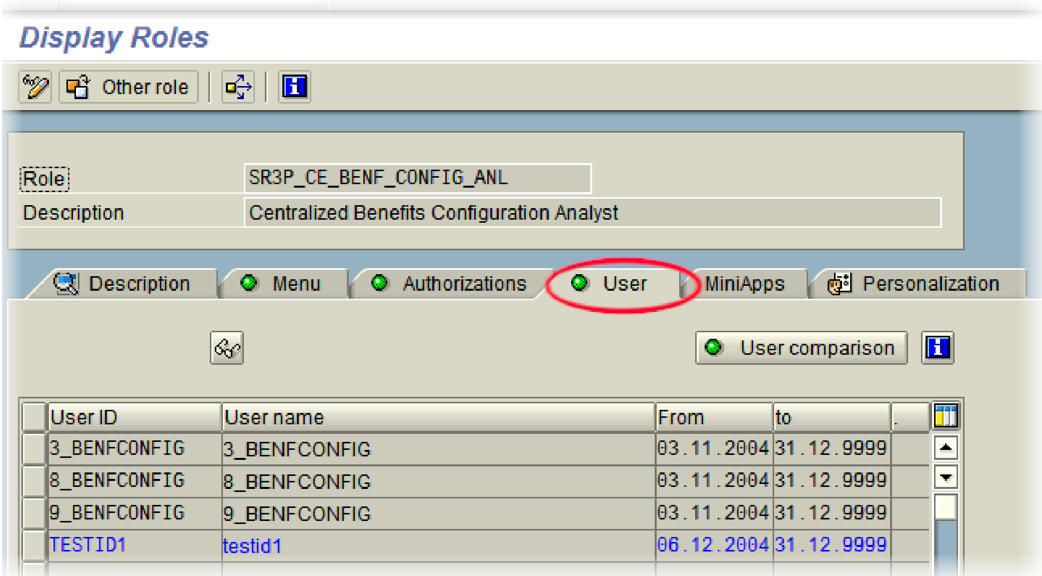
5. The third tab is Authorizations: this additional information about the authorizations for the role. Click on to Display Authorization Data for the role.



6. In the Display role: Authorizations screen, expand the node to view specific authorizations. When finished, click on Back(F3) to return to the Display Roles screen.



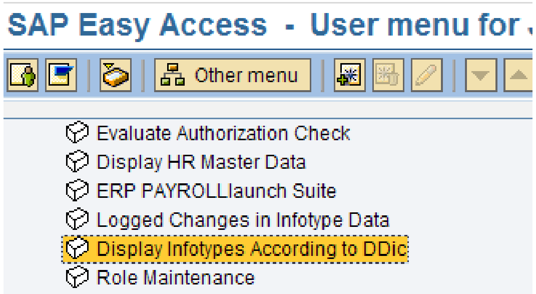
7. The fourth tab is User; this will list users assigned to the role. Direct assignments are noted in Black, Indirect (position based) assignments are shown in Blue.
   NOTE: *The roles should always be assigned to positions.*



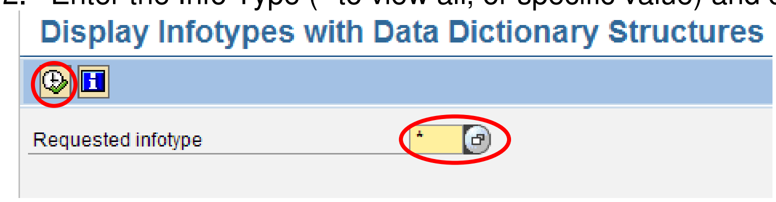
8. The fifth tab is MiniApps and the sixth tab is Personalization. At this time, disregard these tabs.

Display List of Infotypes (S_ALR_87101323)

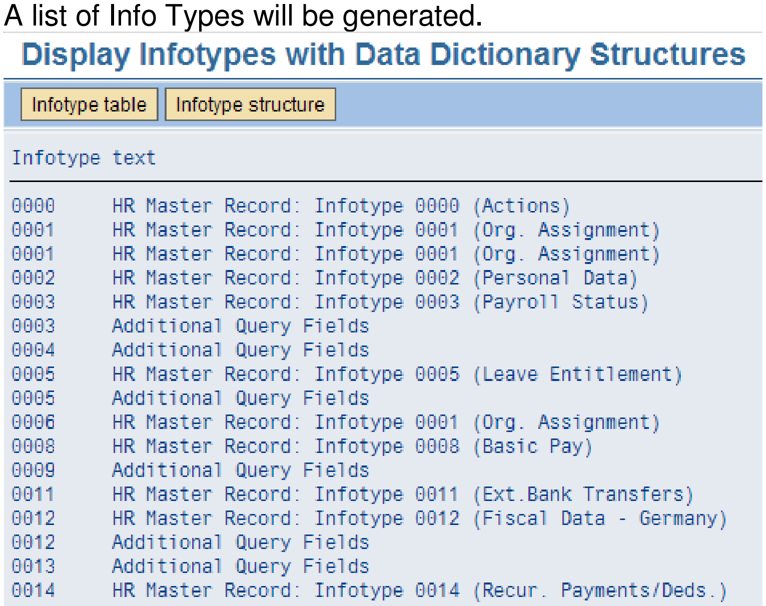
1. Enter transaction '**S_ALR_87101323**' (n/S_ALR_87101323) or select 'Display Infotypes According to DDic' from the main menu.



2. Enter the Info Type (* to view all, or specific value) and click on  to Execute.

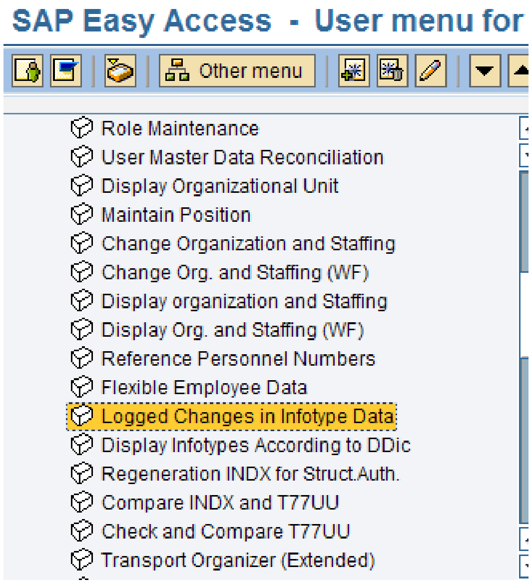


3. A list of Info Types will be generated.

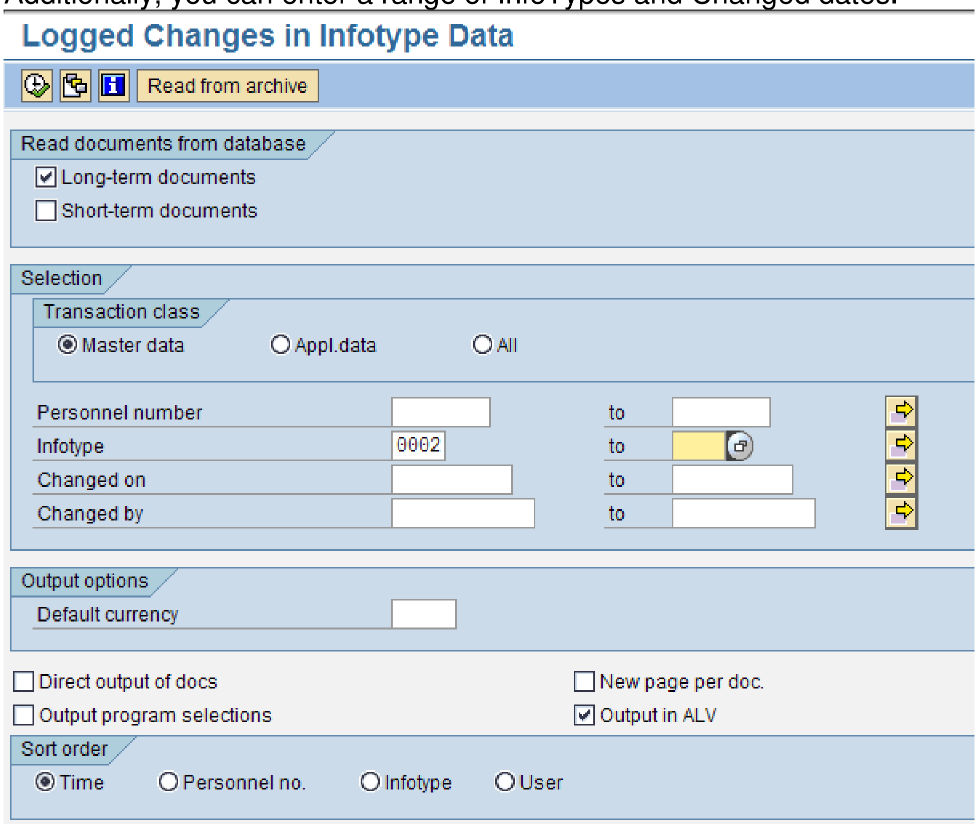


Display Changes in Infotype Data (S_AHR_61016380)

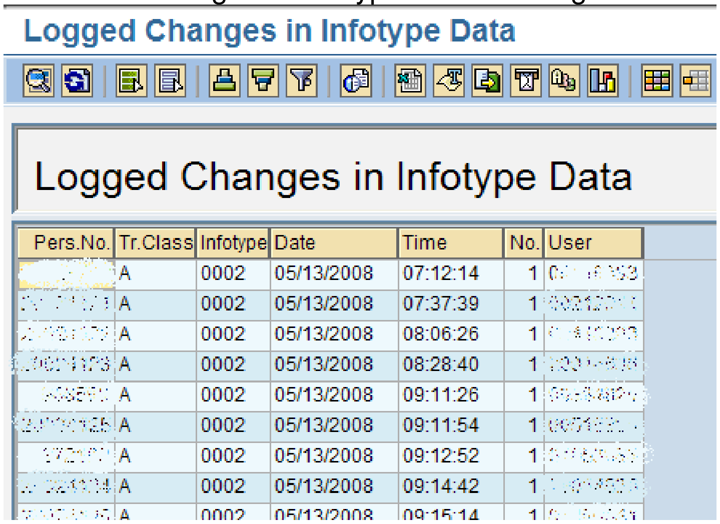
1. Enter transaction '**S_AHR_61016380**' (n/S_AHR_61016380) or select 'Logged Changes in Infotype Data' from the main menu.



2. Select Long-term documents and enter InfoType to search on and click on  to Execute. Additionally, you can enter a range of InfoTypes and Changed dates.



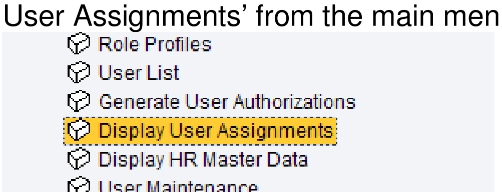
3. A list of Changes in Infotype Data will be generated.



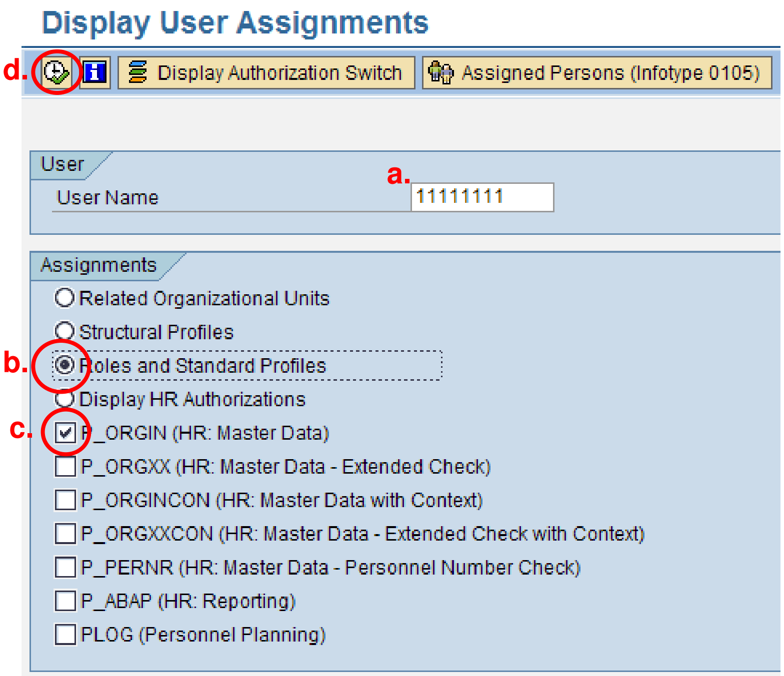
Pers.No.	Tr.Class	Infotype	Date	Time	No.	User
[illegible]	A	0002	05/13/2008	07:12:14	1	[illegible]
[illegible]	A	0002	05/13/2008	07:37:39	1	[illegible]
[illegible]	A	0002	05/13/2008	08:06:26	1	[illegible]
[illegible]	A	0002	05/13/2008	08:28:40	1	[illegible]
[illegible]	A	0002	05/13/2008	09:11:26	1	[illegible]
[illegible]	A	0002	05/13/2008	09:11:54	1	[illegible]
[illegible]	A	0002	05/13/2008	09:12:52	1	[illegible]
[illegible]	A	0002	05/13/2008	09:14:42	1	[illegible]
[illegible]	A	0002	05/13/2008	09:15:14	1	[illegible]

Display User Assignments (ZAUTH_DSP_USR_ASSIGN)

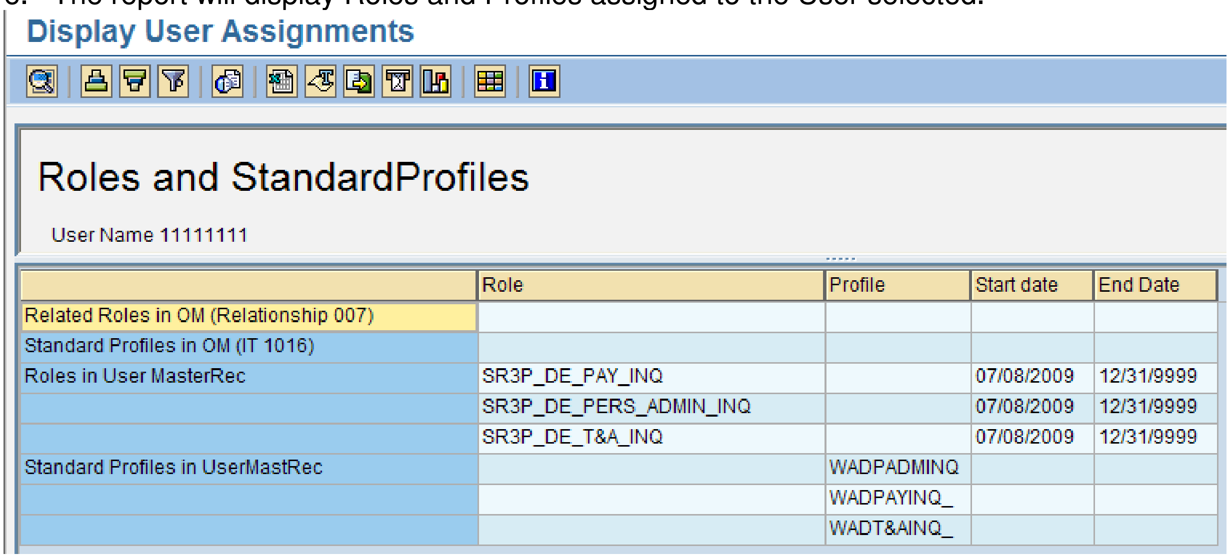
1. Enter transaction ‘**ZAUTH_DSP_USR_ASSIGN**’ (/nZAUTH_DSP_USR_ASSIGN) or select ‘Display User Assignments’ from the main menu.



2. Display Roles and Profiles assigned to User
   a. Enter the UserID into the ‘User Name’ field. The UserID should be the user’s Personnel Number, ***including*** leading zeroes. In this example it is ‘11111111’. To search for the User, click on  to search and select the User.
   b. Select Roles and Standard Profiles
   c. Select P_ORIGIN (HR: Master Data)
   d. Click on  to Execute.

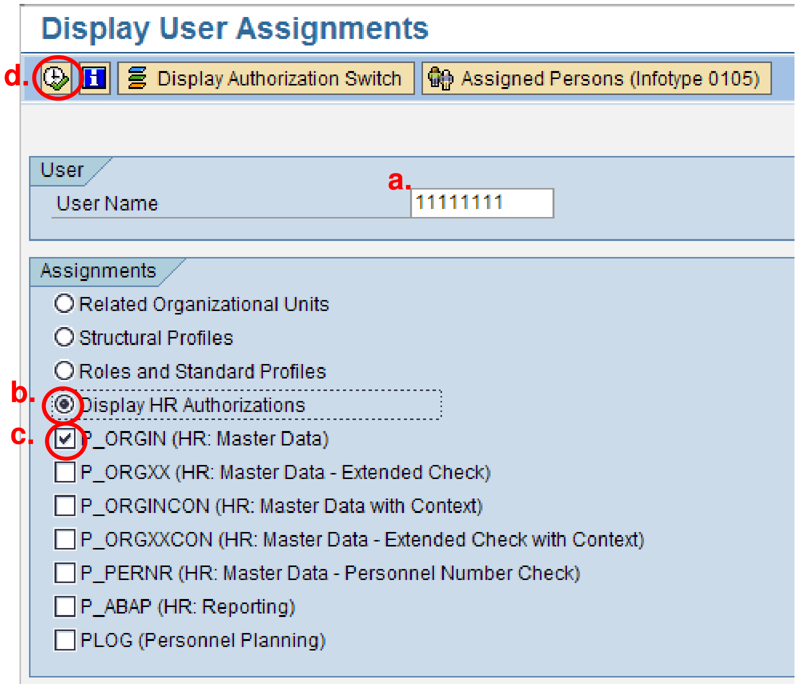


e. The report will display Roles and Profiles assigned to the User selected.

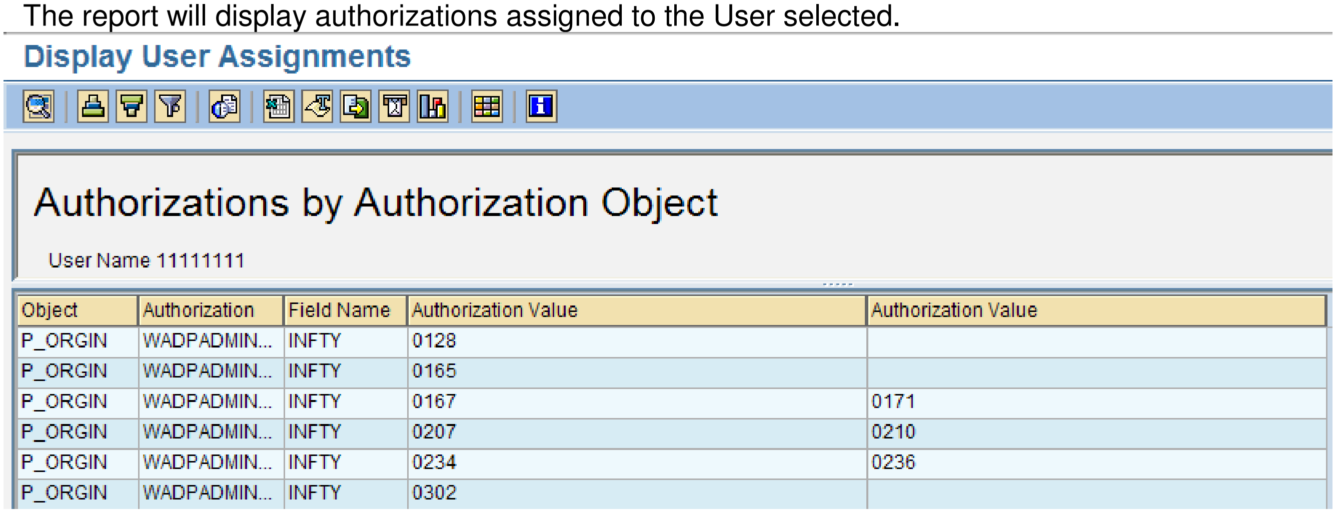


	Role	Profile	Start date	End Date
Related Roles in OM (Relationship 007)				
Standard Profiles in OM (IT 1016)				
Roles in User MasterRec	SR3P_DE_PAY_INQ		07/08/2009	12/31/9999
	SR3P_DE_PERS_ADMIN_INQ		07/08/2009	12/31/9999
	SR3P_DE_T&A_INQ		07/08/2009	12/31/9999
Standard Profiles in UserMastRec		WADPADMINQ		
		WADPAYINQ_		
		WADT&AINQ_		

3. Click the Back button to go back to previous screen.
4. Display HR Authorizations by Authorization Object
   a. Enter the UserID into the 'User Name' field. The UserID should be the user's Personnel Number, ***including*** leading zeroes. In this example it is '11111111'. To search for the User, click on to search and select the User.
   b. Select Display HR Authorizations
   c. Select P_ORIGIN (HR: Master Data)
   d. Click on to Execute.



e. The report will display authorizations assigned to the User selected.



Object	Authorization	Field Name	Authorization Value	Authorization Value
P_ORGIN	WADPADMIN...	INFTY	0128	
P_ORGIN	WADPADMIN...	INFTY	0165	
P_ORGIN	WADPADMIN...	INFTY	0167	0171
P_ORGIN	WADPADMIN...	INFTY	0207	0210
P_ORGIN	WADPADMIN...	INFTY	0234	0236
P_ORGIN	WADPADMIN...	INFTY	0302	

BI (Business Intelligence) ZS_BI_XXXX_USER_ADMIN

Introduction

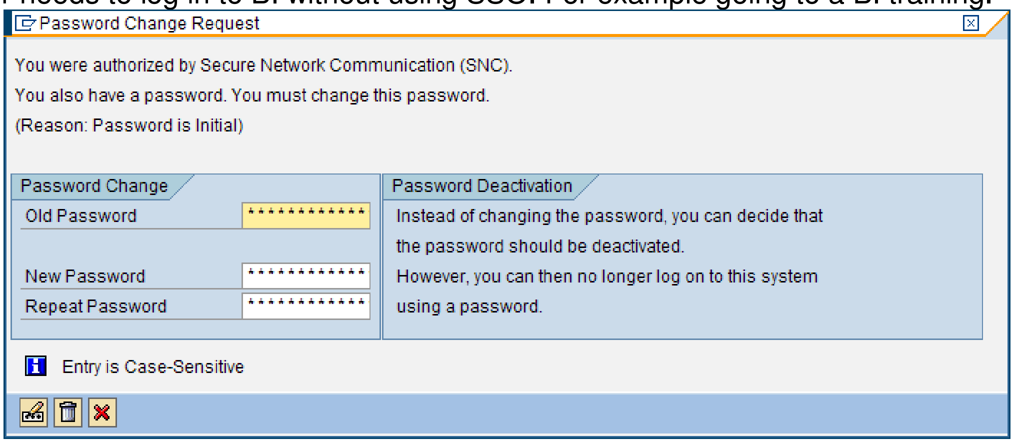
All BI Users must first have an HCM Authorization Profile assigned through the OOSB (Table T77UA). BI UserIDs will have access to retrieve data on the next business day following the creation of their UserID and role assignment(s).

There are two types of BI Reporting Users:

- END_USER: This type of user will retrieve data from BI through the HRMS Portal ***or***
- POWER_USER: This type of user will retrieve data directly through BI

BI Users will need UserID & password to display query results on the web (execute WBWT template).

When SSO users login to BI for the first time the system will ask the user to either change the initial password or deactivate it. Our recommendation is **to change the password** and keep a note of it, in case the user needs to log in to BI without using SSO. For example going to a BI training.



NOTE: *Changing initial BI password will **not** affect logging in to the portal using SSO with a professional LDAP account. This type of account requires the user to input their network password.*

Also, BI UserID accounts are created for:

- Access HCM professional roles through the HRMS Portal with the use of WebGui. Information on how to assign an WebGui group role to the Portal Professional account can be found in the HRMS Portal chapter of this handbook.

Maintaining a Professional BI UserID Account

Create BI UserID (SU01)

Prerequisites:

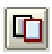
- ✓ UserID is created in HCM, has at least XXXX_Data_Profile role.
- ✓ The Authorization Profile assigned through the OOSB in HCM (not required for Professional BI Users)

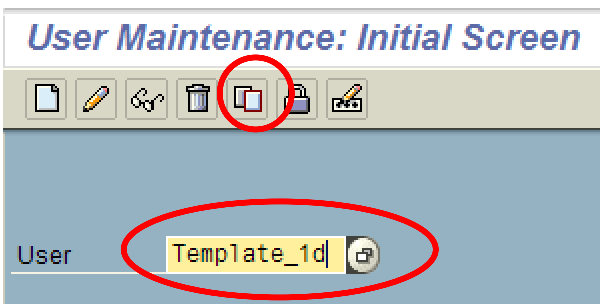
1. Login to the BIP environment (HRMS Business Intelligence);

2. Enter transaction '**SU01**' (/nSU01) to create BI UserID

3. Copy the model UserID "Template_1D" to create the new UserID.

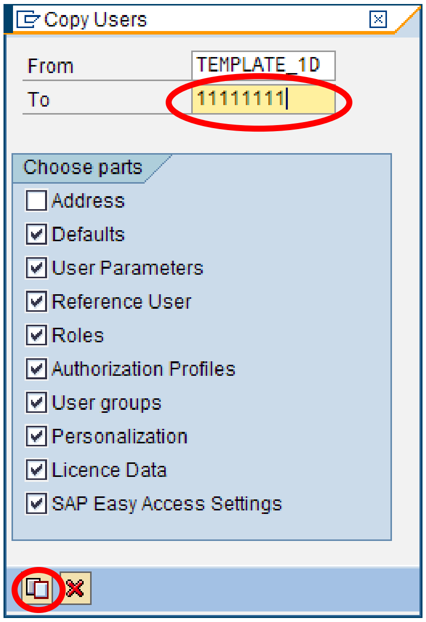
   a. Enter TEMPLATE_1D in the 'User' field.

   b. Click on  to COPY the Template UserID.

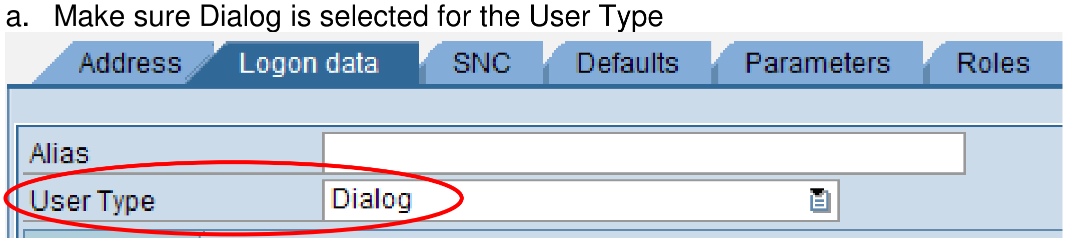


NOTE*: The TEMPLATE_1D UserID was created to assist in the creation of new UserIDs. This ID contains basic default settings that all UserIDs will need. There are several fields that will require changes after the copy is performed and before the UserID will be useable in the system.*

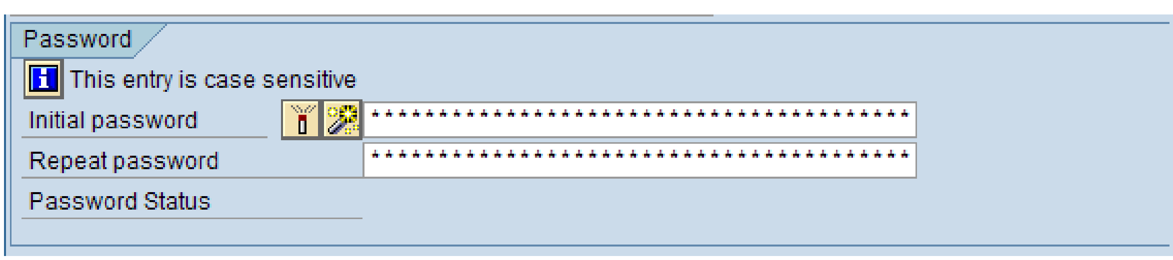
4. Enter the new UserID (Personnel number, ***including*** leading zeroes to create an eight digit UserID. This must match the UserID in HCM – HRMS Production) and click on (Copy) to continue.



5. From the ‘Logon data’ tab, update the following:
   a. Make sure Dialog is selected for the User Type



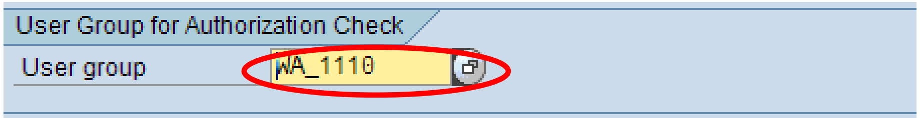
   b. Click in the initial password field and type in an initial password and then retype the same password in the Repeat Password field. Note that ‘hardened’ password standards apply (i.e. must contain at least 1 letter, 1 number and 1 special character, and must be at least 8 characters long). DO NOT click on the wizard button. This will generate a 40 digit password.



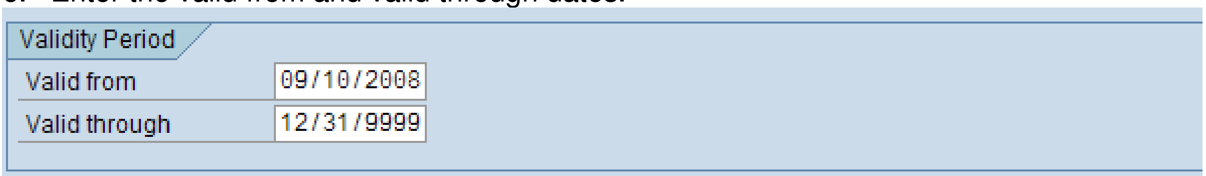
   c. Make note of the password for distribution to the BI User and to map the BI account to the HRMS Portal account if needed.

NOTE*: All BI Users will need UserID and password to display query results on the web. The (SSO) BI User should always use the SSO button on the SAP GUI logon pad.*

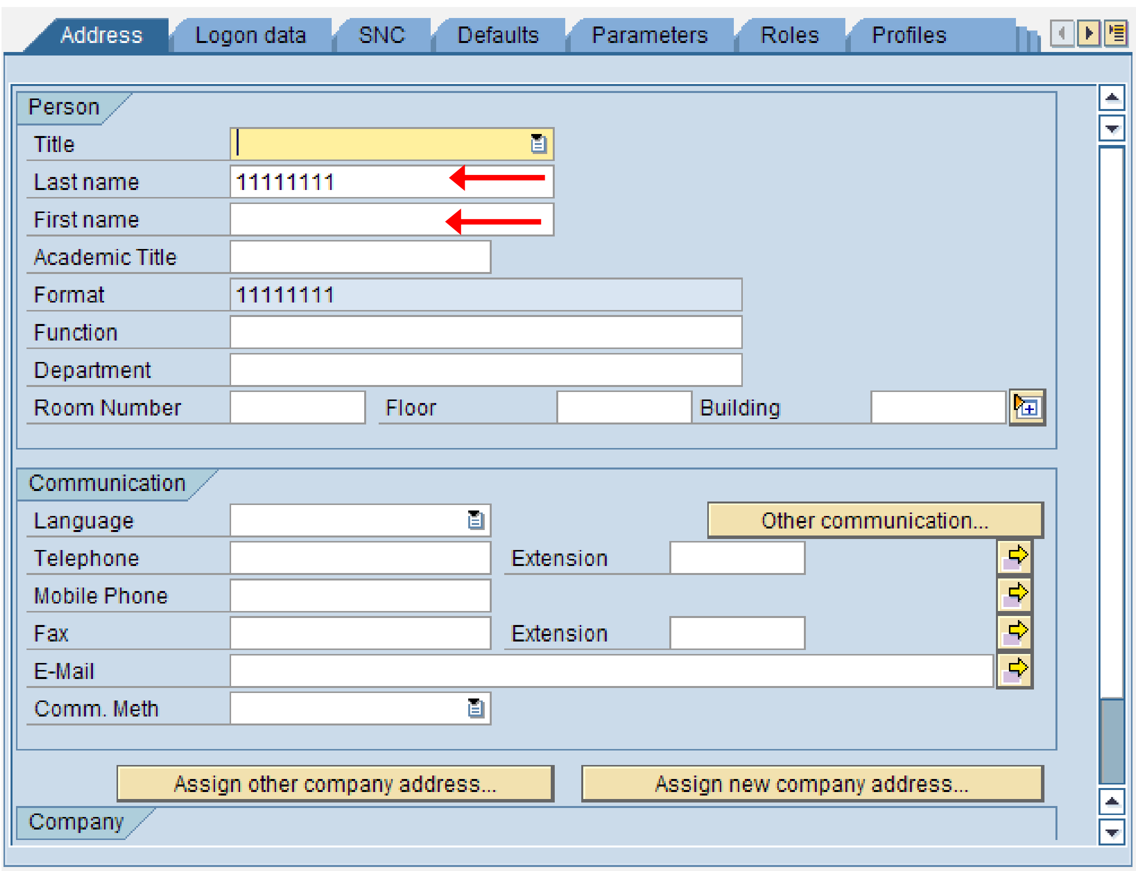
d. Enter the User Group for your Agency. To search, click on the button to search for your User Group.



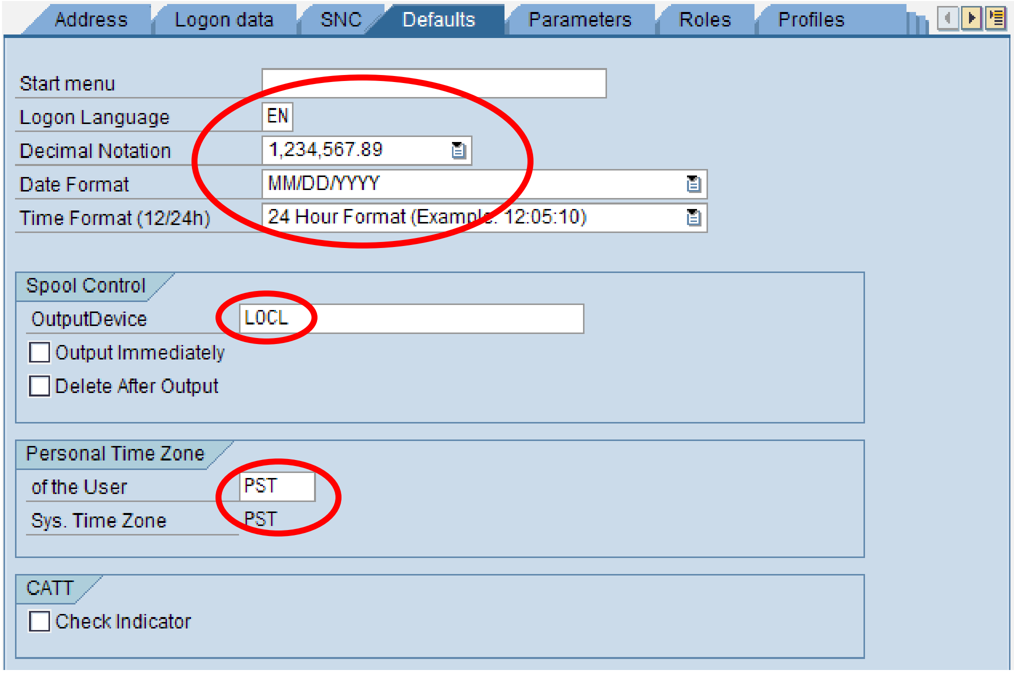
e. Enter the valid from and valid through dates.



6. Select the 'Address' tab, enter user's first and last name and any other desired information and press enter when complete.



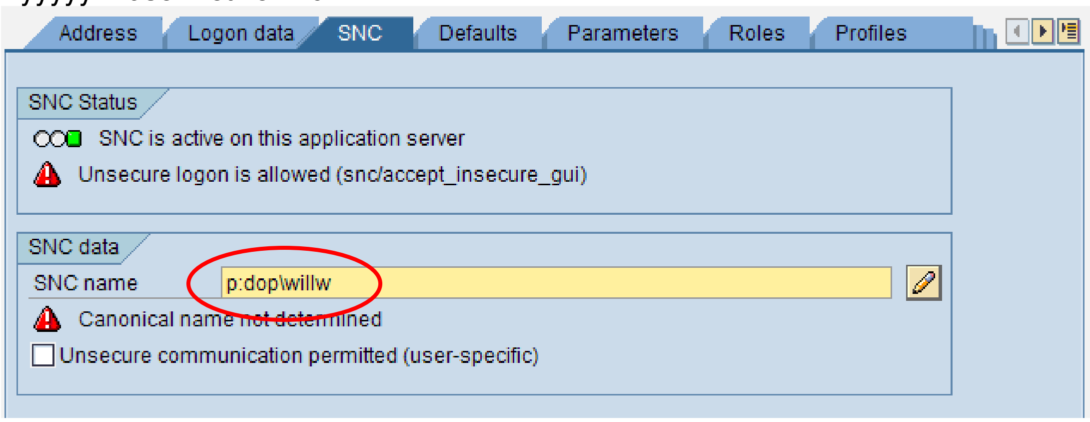
7. Click on the ‘Defaults’ tab. If you did ***not*** copy this UserID from ‘Template_1D’, ensure the following fields are filled as shown:



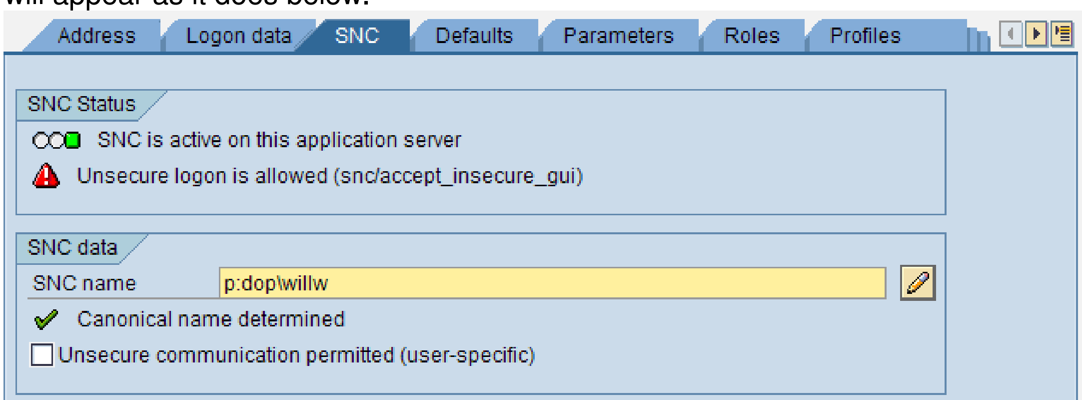
If NOT using Single Sign On (SSO) you are done. If you ARE using SSO continue to step 8.

Single Sign On

8. Click the “SNC’ tab. Enter the SNC name in the following format ‘p:xxx\yyyy’ (see example below).
   - xxx = 3 letter agency code
   - yyyyy = user network id



9. If the update is successful, a green check mark and the message “Canonical name determined” will appear as it does below.



10. Click on (Save) when finished.

Assign Professional Roles to a BI UserID Account (SU01)

NOTE*: The GENERAL ACCESS role MUST be assigned to all BI user accounts. For assigning multiple users, Mass UserID Maintenance (SU10) can also be used.*

<u>Roles for BI UserIDs</u>

BI users will need the following roles:

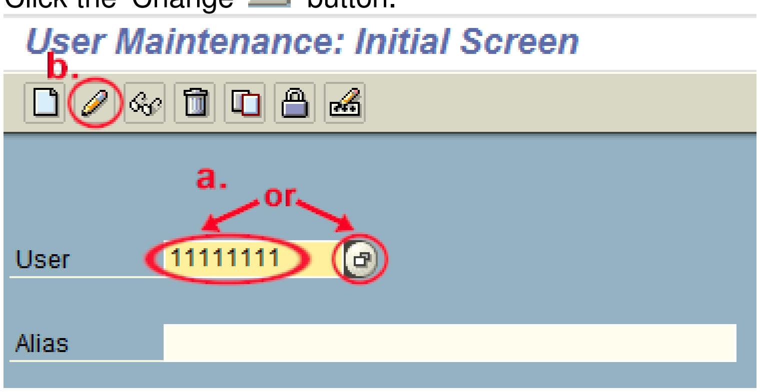
- ZS_BI_GENERAL_ACCESS (Contains general use transactions),
- ZS_BI_XXXX_END_USER ***or***
- ZS_BI_XXXX_POWER_USER (where 'XXXX' is your personnel area)
- ZS_BI_XXXX_WBWT Agency Workbook/Web template)
- ZS_BI_SOW_WBWT (State of Washington Workbook/Web template)

and one <u>OR</u> more of the following

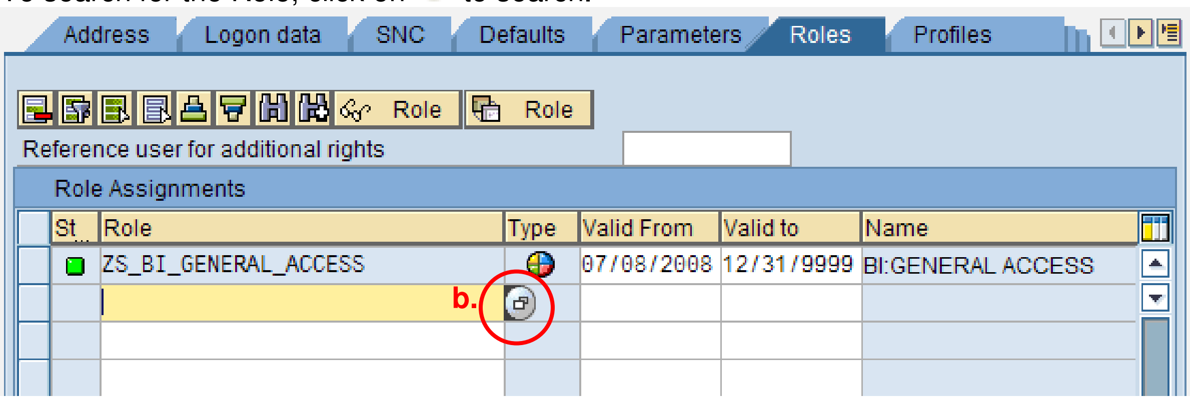
- ZS_BI-FI_ANALYSIS (Access to Financial data)
- ZS_BI-HR_ANALYSIS (Access to HR data)
- ZS_BI-GR_ANALYSIS (Access to Grievance data)

Roles in BI are assigned directly to the UserID.

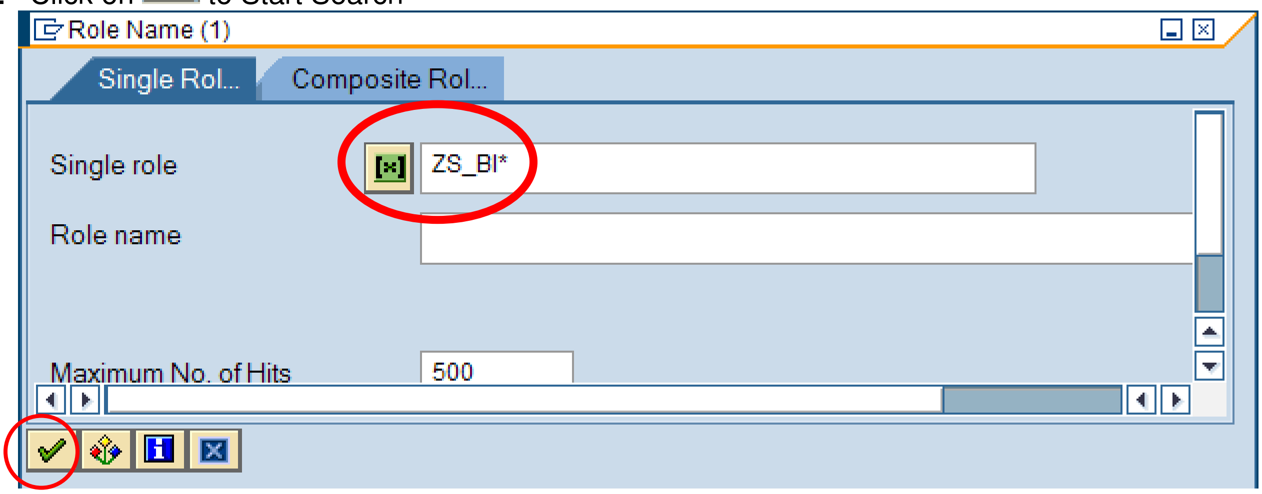
1. Log into BIP (HRMS Business Intelligence);
2. Enter transaction '**SU01**' (/nSU01) to Assign Role(s) to UserID(s)
3. Enter/Search for the UserID.
   a. Enter the UserID (8 digit Personnel Number, ***including*** leading zeroes) into the 'User' field. In this example it is '11111111'. To search for the User, click on to search and select the User.
   b. Click the 'Change' button.



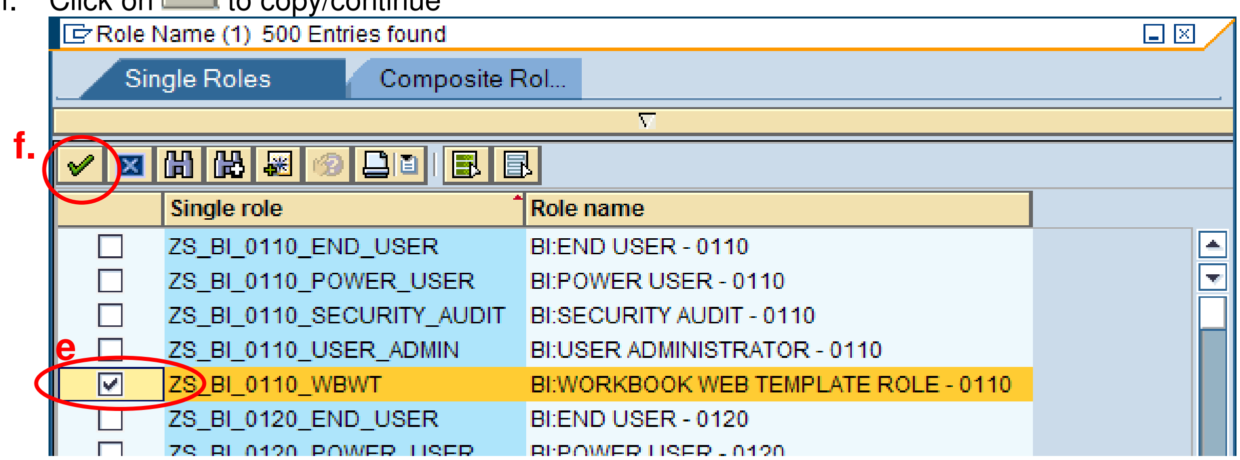
3. Click the ‘Roles’ tab, enter the Role name.
   a. If you know the role, type it in the first empty cell and press enter.
   b. To search for the Role, click on to search.



   c. Enter ZS_BI* in the ‘Single Role’ field
   d. Click on to Start Search



   e. Select the role(s) desired and place a checkmark in the box to the left.
   f. Click on to copy/continue

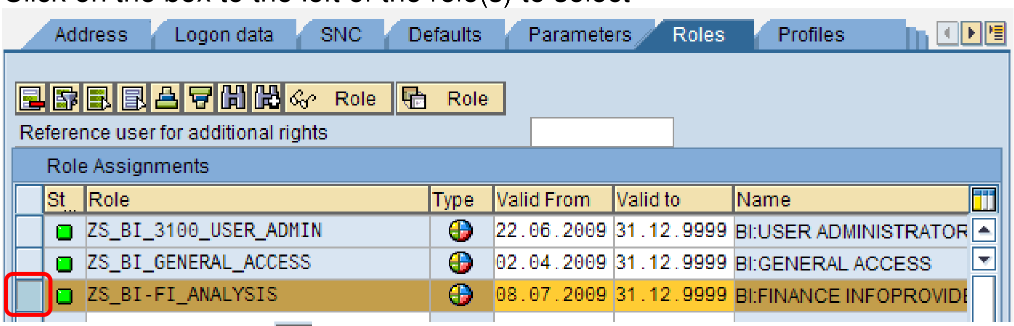


   g. Repeat as necessary to add any additional roles.

1. Close the Display Role screen.
2. Repeat from step 4 for any other roles.

Delete Professional Roles from a BI UserID Account (SU01)

1. Log in to BIP (HRMS Business Intelligence)
2. Enter the UserID (8 digit Personnel Number, ***including*** leading zeroes) into the ‘User’ field.
3. Click on the Display button, and verify the user.
4. On the Roles tab; Click on Display/Change button to enter the edit mode.
5. Click on the box to the left of the role(s) to select



6. Click on Delete Row button to delete the role(s)
7. Click the Save button to save the account.

BI UserID Maintenance

For the complete steps of maintenance processes, refer to the previous chapter HCM UserID Maintenance. The steps are the same in BI as they are in HCM.

Reset BI Password (SU01)
Lock/Unlock BI UserID (SU01)
Mass BI UserID Lock/Unlock (SU10)

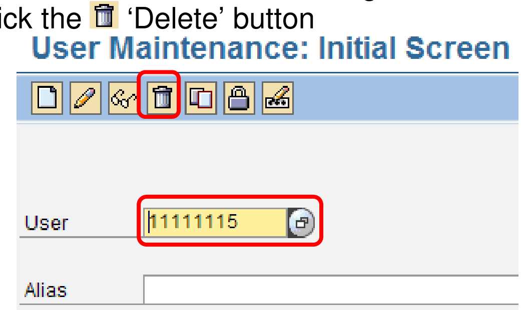
Some of the options where the SU10 Mass User Maintenance transaction might be more effective than one-at-a-time changes are:

- locking of UserIDs,
- changing Parameters and/or Defaults,
- assigning common roles to a large group

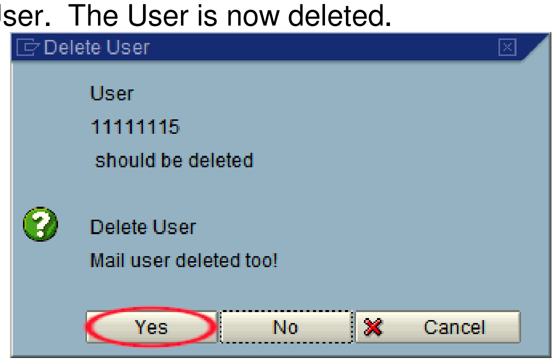
Professional Users Transfer out of the Agency or Professional Users Become Non-Professional Users (ESS Users):

BI:

1. Log into BIP – Business Intelligence Production – through the SAP Logon Pad
2. Enter transaction '**SU01**' (/nSU01) to delete the UserID.
3. Enter the UserID (8 digit Personnel Number, ***including*** leading zeroes) into the 'User' field. In this example it is '11111115'. To search for the User, click on to search and select the User.
4. Click the Display button to verify the user
5. Click on the Back button to go back to the User Maintenance screen
6. Click the 'Delete' button



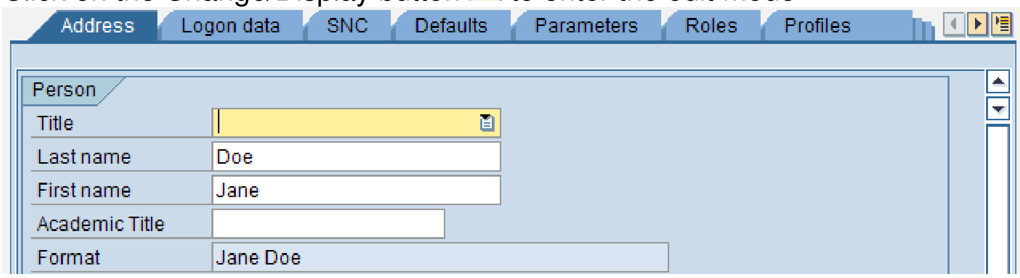
7. A screen like the one below will appear. Click the 'Yes' button if you are sure you want to delete the User. The User is now deleted.



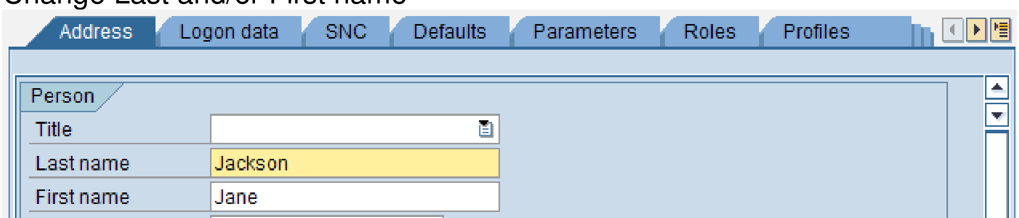
Employee has a Name Change

NOTE: *When an employee has a name change and the HCM personnel master record is updated, this change does not update the UserID account (SU01) for that employee in BI. The Agency User Administrator must manually go into SU01 and change employee's name.*

1. Enter transaction SU01
2. Enter the UserID (8 digit Personnel Number, ***including*** leading zeroes) into the 'User' field
3. Click the Display button to verify the user
4. Click on the Change/Display button to enter the edit mode



5. Change Last and/or First name



6. Click on Save to save the account.

HRMS Portal – User Admin

Introduction

There are three types of Portal Logon ID's:

1. Personal ESS User Logon ID - Created by Department of Personnel (DOP). **The Logon ID is the user's 8 digit Personnel Number**. This Logon ID may be locked, unlocked or have its password reset by the Agency's Portal User Administrator(s).

2. Professional LDAP Logon ID - Users accessing the Portal who are connected to the state's Active Directory tree will be granted Portal access based on their email address and network password. **The Logon ID is the user's agency email address.** Password resets for these are the responsibility of the agency network admins.

3. Professional UME Logon ID - Created by the agencies' Portal User Admins. **The Logon ID is the user's agency domain\network username (dop\warrenk).** These accounts require maintenance by the agency User Admins, including creation, deletion, password resetting, locking and unlocking of the accounts, and role/group assignments.

Logon to the HRMS Portal

1. Logon to the HRMS Portal from work; open your web browser and enter this URL if your agency is in the Enterprise Active Directly (*INSIDE* the State Government Network) https://myhrms.wa.gov/irj

2. Logon to Portal from work, home or anywhere outside the State Government Network (SGN) enter: https://wahrms.wa.gov/irj

- Inside the SGN (In the Active Directory) - enter your work email address (like warrenk@dis.wa.gov) as your Logon ID to enter the secure (HTTPS) portal. Use your normal network password to login. If the agency is single sign-on (SSO), users should go directly into the portal. (If you are logging in outside of the SGN you would still use your email address and network password).

- Outside the SGN - If you normally have to log into the Portal using your agency domain\network username (like dis\warrenk) there will be no difference in Logon ID or password from any location.

Professional Portal Accounts

There are two ways to setup access for a user in the Portal. This depends on whether or not your agency is connected to the State Government Active Directory:

1. If you are IN the State Government Active Directory, your employee's accounts are already created in the portal. The user's email address is his/her Portal Logon ID. Logging into the portal is based on the user's email address and network password and could also possibly be Single Sign On (SSO).

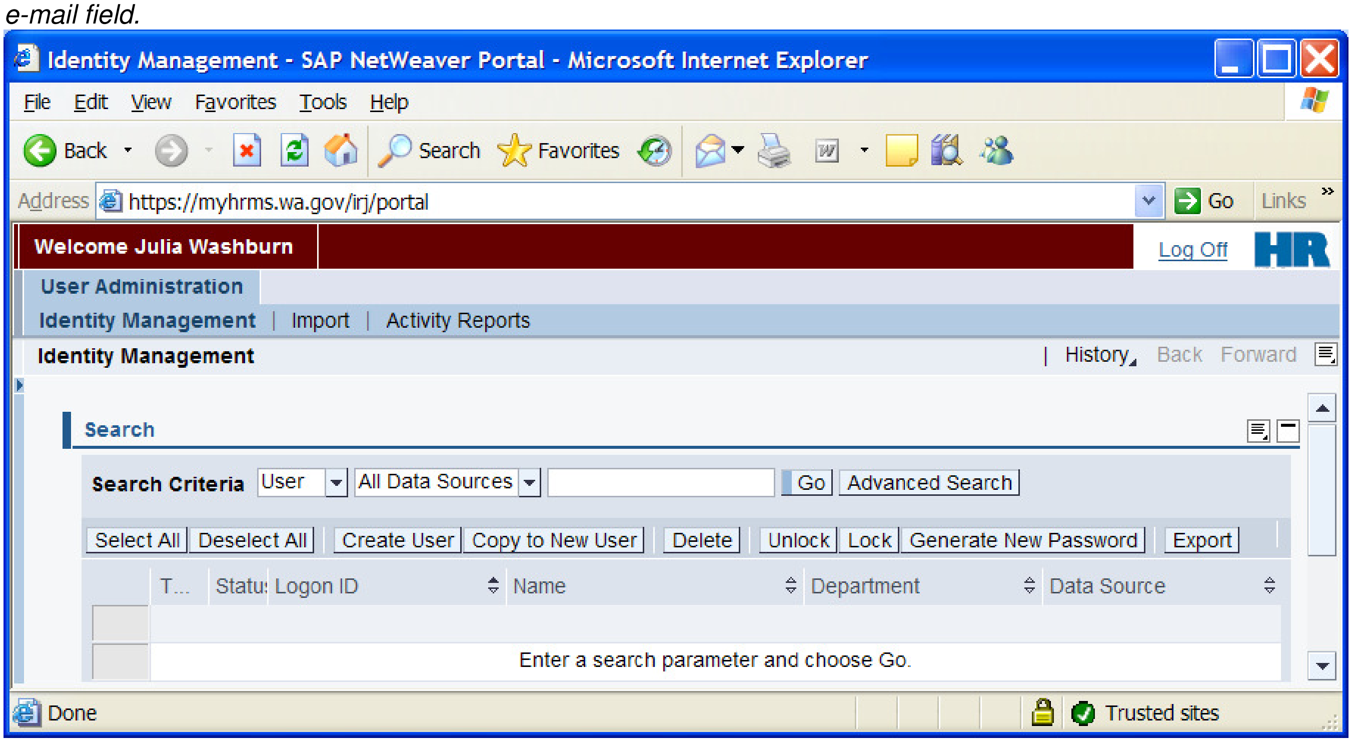
2. If you are NOT a member of the State Government Active Directory, you must Create/Delete your agency Professional Portal UserID/Logon IDs and manage their passwords.

As a Portal User Administrator, you may:

a. <u>Assign the User_Admin SINGLE role.</u> (*User* Admin*)
b. <u>Assign the HR_HtmlGui_GRP GROUP role.</u> (Access to HCM through the WEBGUI)
c. <u>Assign the BI_Reports_GRP GROUP role.</u> (Access to BI reports)
d. <u>Map the Portal Logon ID to BIP UserID Account</u>.

The image below shows the HRMS Portal. You should at LEAST have the "User Administration" tab shown, and the "Identity Management" sub-tab also selected. Many actions can be initiated from this screen directly: *Create User*, *Delete*, *Lock/Unlock*, and *Advanced Search*. We recommend using the "Advanced Search" option if you do not know the exact Logon ID.

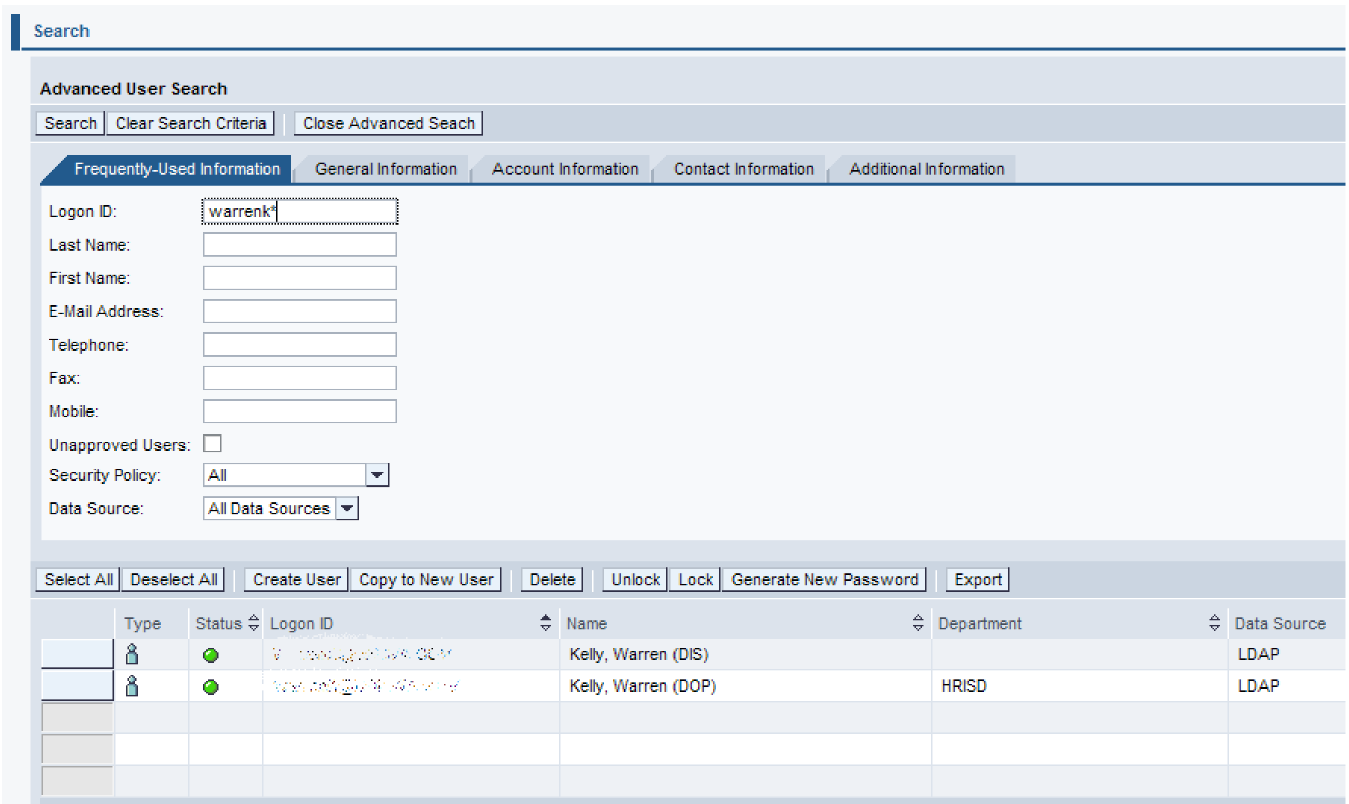
NOTE*: To search for the e-mail address as a Logon ID you have to use the Advanced Search and search by the e-mail field.*



Advanced Search

Select the “Advanced Search” option on the Identity Management screen. This will take you to the following screen:

1. Search for a user by the Logon ID, Last Name, First Name or E-Mail Address
   Hint: When searching you may substitute the asterisk in any character position to represent unknown characters or wrap known characters around multiple asterisks. (EX: warrenk*; *@*.wa.gov)
2. Click the Search button. You will see the screen similar to the one shown below.



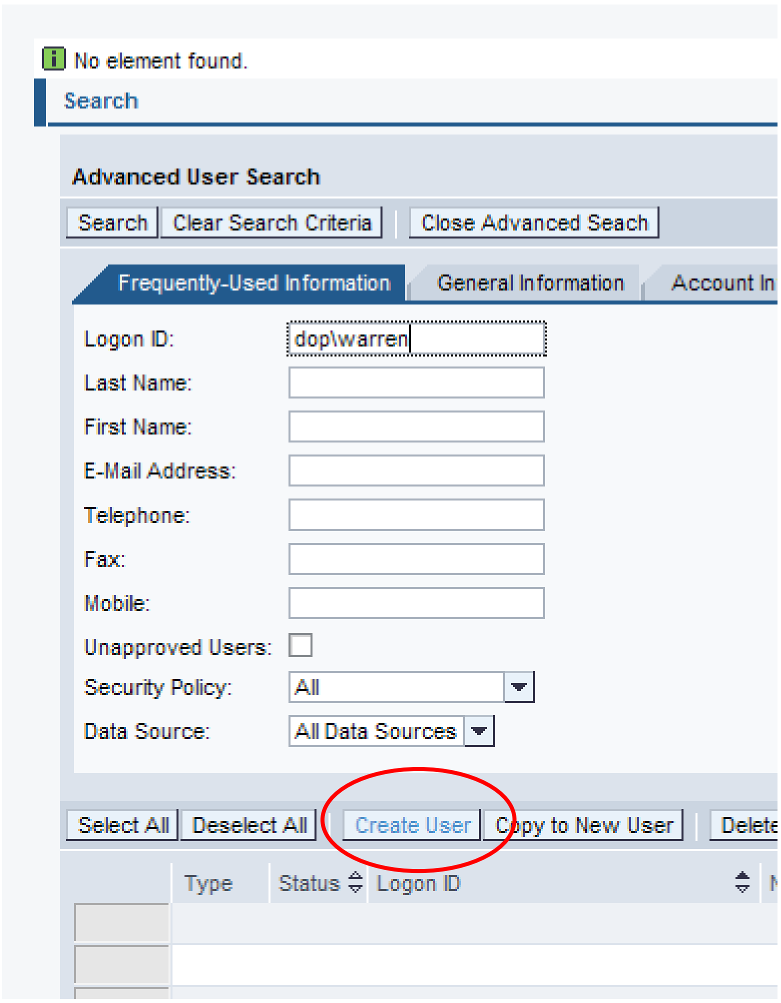
3. Click on the user you need. The selected user will be highlighted and the Details view will be shown.

Advanced Search can be used to find all types of Portal user accounts: ESS, Professional LDAP (e-mail) and Professional UME (domain\network username)

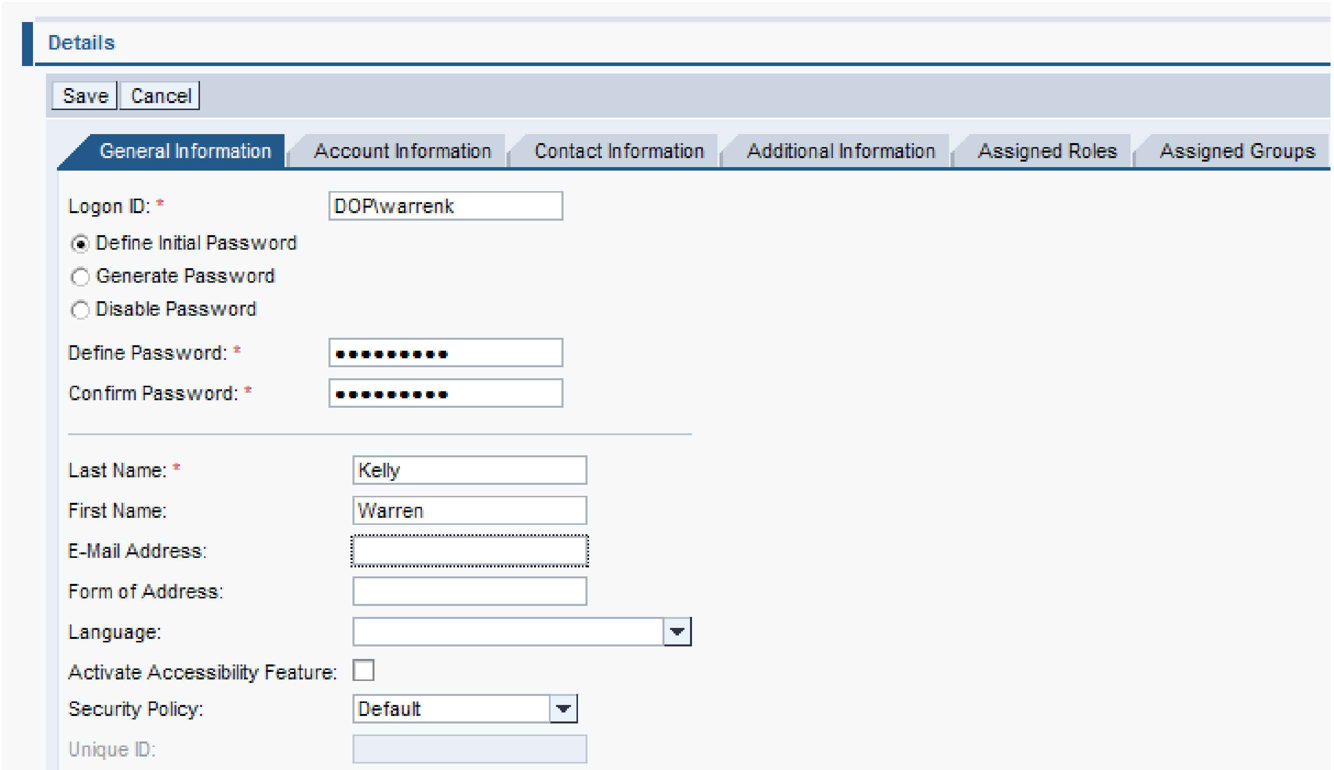
Maintaining a Professional Portal Logon ID Account

Creating Professional Portal Logon IDs (UME)

NOTE: *If you are in the Active Directory and/or a Single Sign On (SSO) agency you do not need to create Professional Portal accounts. They are created automatically and the login ID is the e-mail address. To login to those accounts you will need to use your network password. You will only need to assign groups/roles to those accounts and map to the BI account.*



1. Click on the “Create User” button (circled in red above) and your screen format will change to what is shown below:



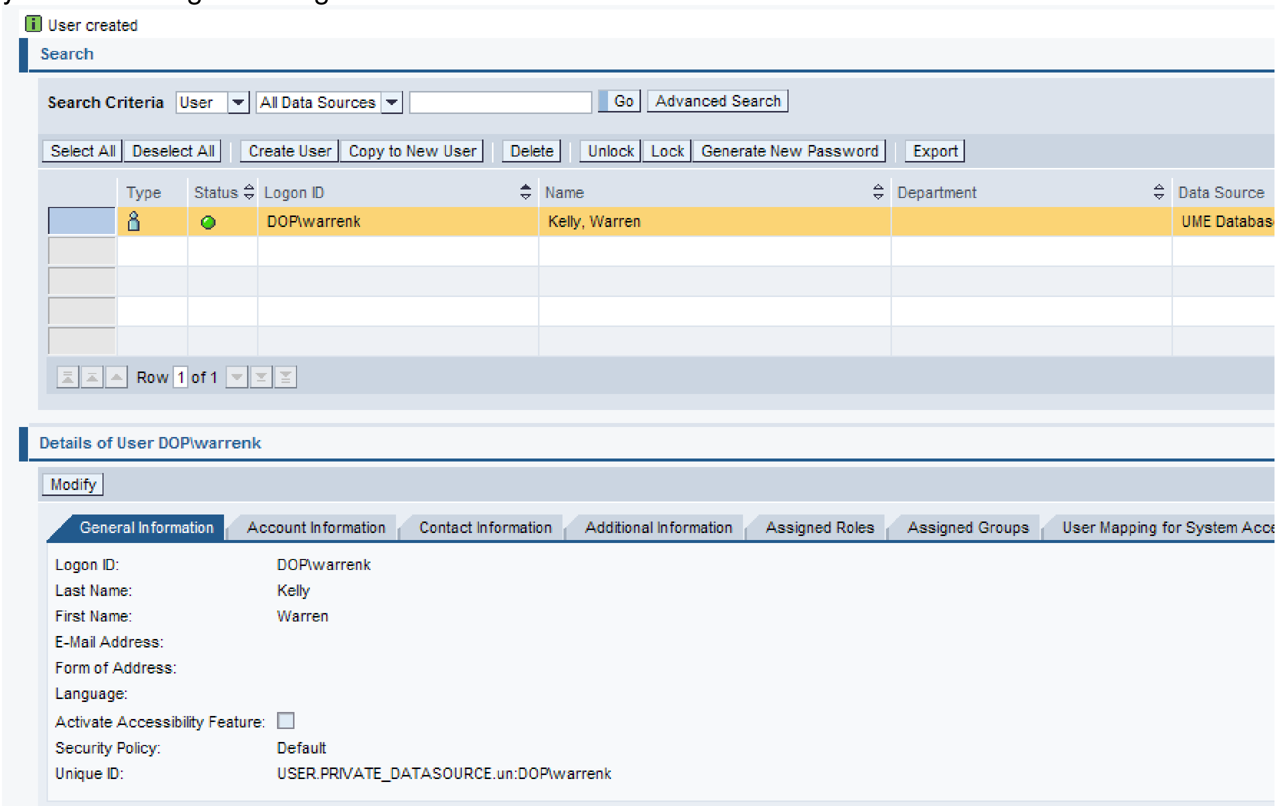
2. Fill in the data as shown:

- Logon ID - Using your Agency's domain (DOP in this case) slash (\) username (EX: DOP\warrenk)

- Password – enter your own. The initial password can be any generic password. The user will change it to his/her own hardened password at the first log in.

- Last Name and First Name.

3. Click Save. Clicking on the “Save” button will create the UserID/Logon ID. Once you’ve done this, you can manage this Logon ID.



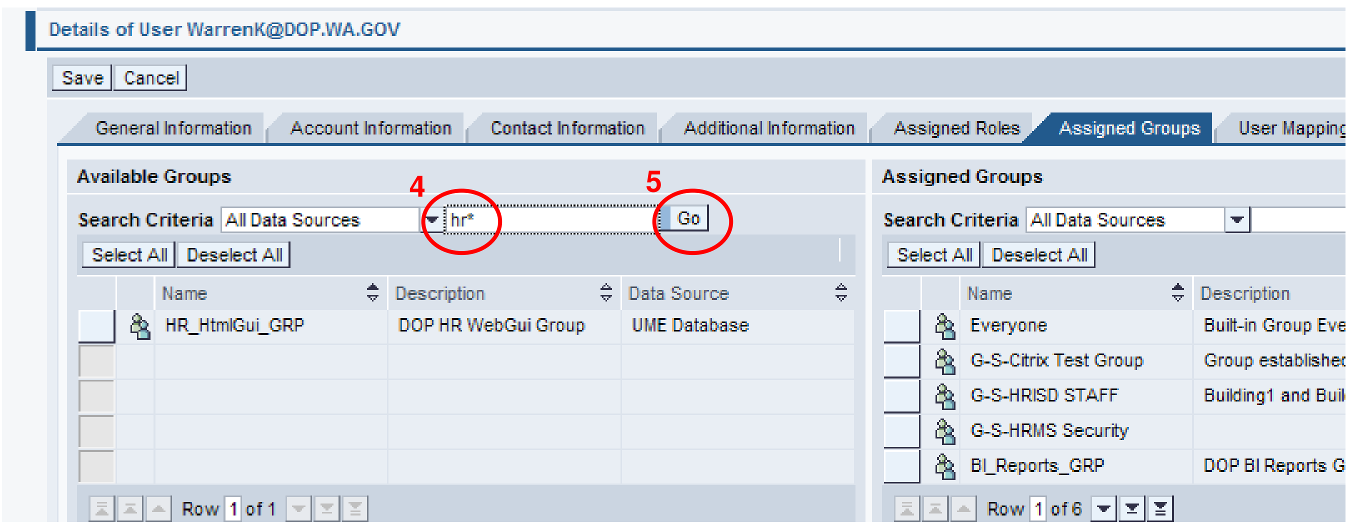
Assigning Group Roles to Professional LDAP or UME LogonID's

1. Search for a user using the Advanced Search described earlier, select it for editing.
2. Click on the Assigned Groups tab. You will see all the groups that are already assigned to the user. This will include default groups, and distribution lists.
3. Click on the Modify button to enter the edit mode.
4. Search for the Group to assign to the user in the Available Groups section. Enter the full name of the group or a part of the name with wildcards such as HR*
5. Click the Go button. This will show all the Available Groups that meet the search criteria (HR_HtmlGui_GRP in this example)

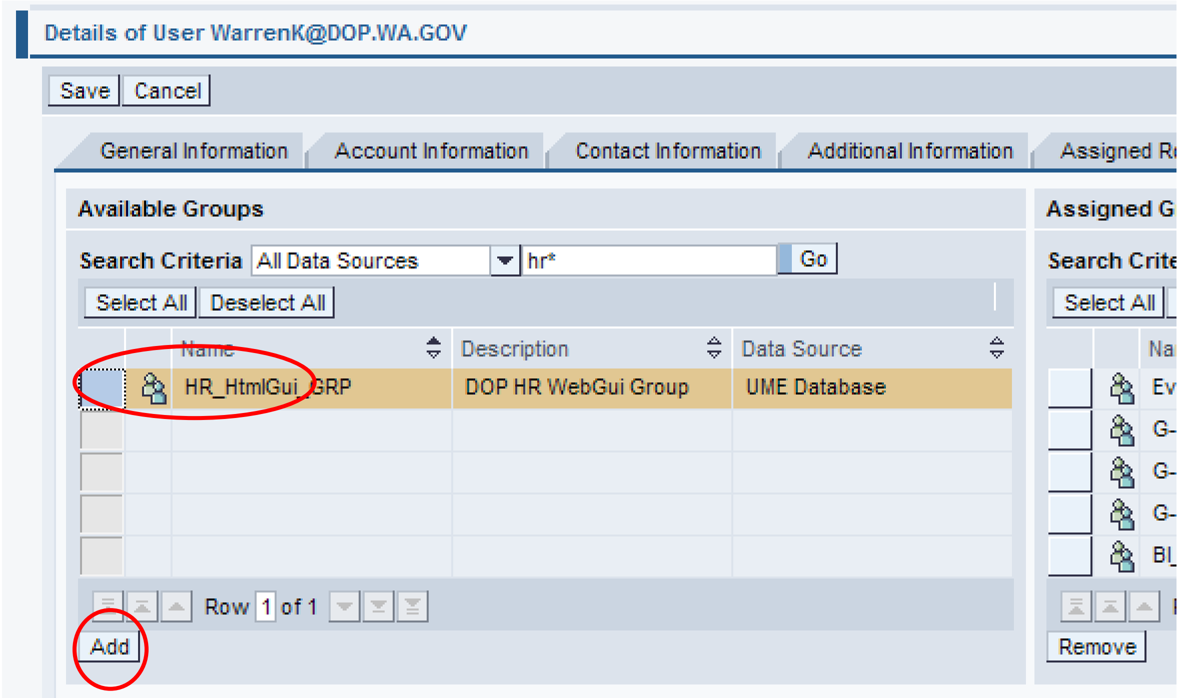
   Available Portal GROUP Roles.

   Portal BI Reporting GROUP Role:
   - BI_REPORTS_GRP

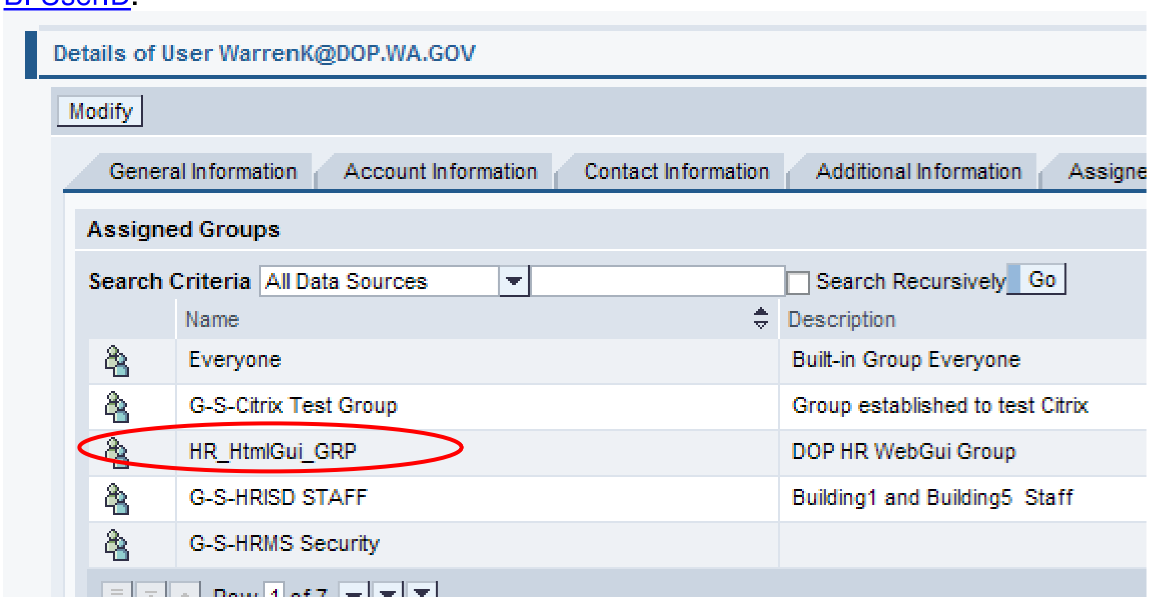
   Portal WEBGUI GROUP Role:
   - HR_HtmlGui_GRP



6. Click the box to the left of the Group name to select it. The row will be highlighted.
7. Click the Add button to add the Group role to the Assigned Groups section.



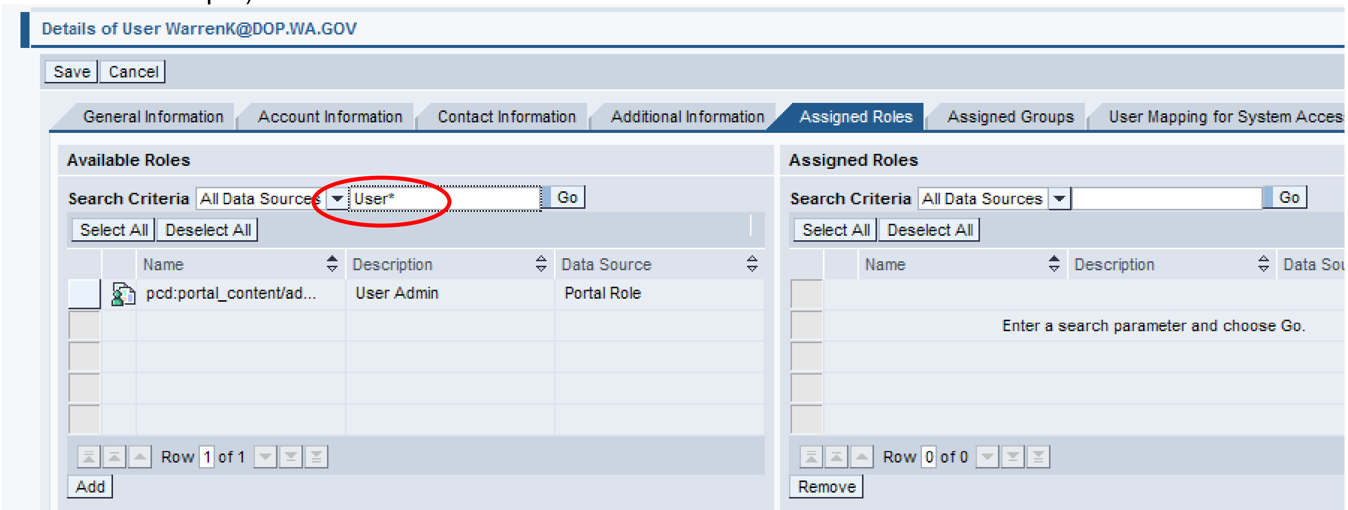
8. Search and assign any additional Group roles if needed. Steps 4 - 7
9. Click the Save button to save the changes to the user account. The newly assigned Group Role(s) will be shown in the "Assigned Groups"
10. You will also need to user map the Portal account to the BI account. [Please refer to the Mapping to BI UserID](#).

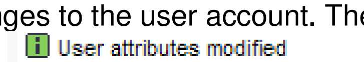


Assigning User Admin Single Role to Professional LDAP or UME LogonID's

1. Search for a user using the [Advanced Search](#) described earlier, select it for editing.
2. Click on the Assigned Roles tab.
3. Click on the Modify button to enter the edit mode.
4. Search for the User Admin role to assign to the user in the Available Roles section. Enter *User*Admin* in the criteria field

5. Click the Go button. This will show all the Available Roles that meet the search criteria (User Admin in this example). Choose the **User Admin** role.



6. Click the box to the left of the role name to select it. The row will be highlighted.
7. Click the Add button to add the User Admin role to the Assigned Roles section.
8. Click the Save button to save the changes to the user account. The User Admin Role will be shown in the "Assigned Roles". The message 

will appear at the top of the screen.

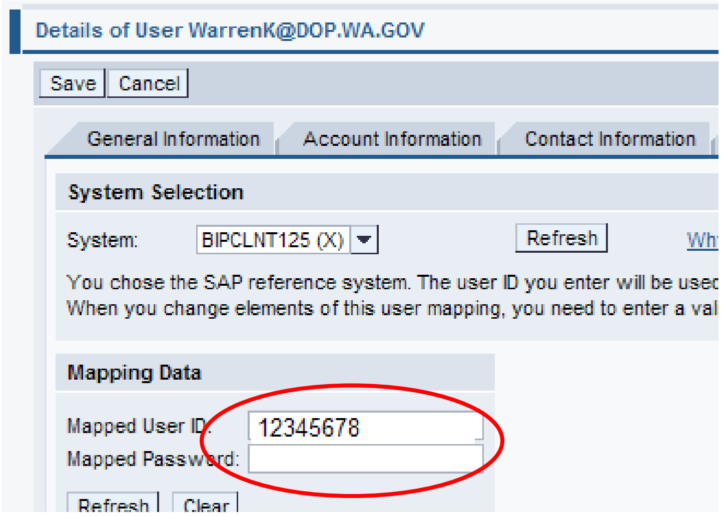
Mapping to BI UserID

NOTE: *The Professional Portal accounts need to be mapped to BI UserID accounts when the Professional Portal account has BI_Reports_GRP and/or HR_HtmlGui_GRP group.*

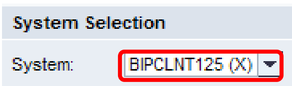
***Effective April 26, 2010 you MUST also contact the DOP Service Center to have Professional Portal accounts mapped to the Federated Portal. You will need to provide the BI UserID and current password and the Professional Portal account userID (LDAP or UME). Send requests to the DOP Service Center at servicecenter@dop.wa.gov or contact 360-664-6400.*

1. Search for a user using the Advanced Search described earlier, select it for editing.
2. Click on the User Mapping for System Access tab.
3. Click on the Modify button to enter the edit mode.
4. Enter the BIP UserID (8 digit personnel number including leading zeros) into the Mapped UserID field
5. Enter the BIP password for the UserID in the Mapped Password field
   NOTE: *You will have to know the user's BIP password. Most likely it will be the initial password that a BI User Admin created. If it is a productive password, BI User Admin should either reset it or ask the user for their productive BI password.*
6. Click the Save button. The message 

will appear at the top of the screen.



7. After a successful mapping you will see an **X** in the System drop down box BIPCLNT125 (**X**)



8. Remember to contact DOP to have the userid mapped in the Federated Portal!

Portal LogonID Maintenance

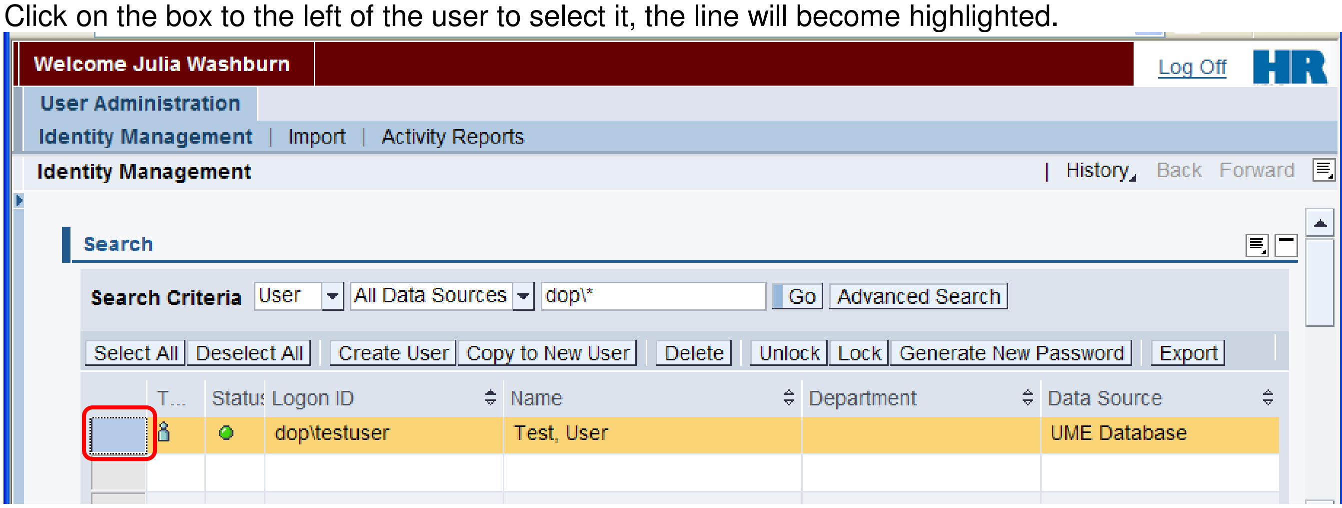
Reset Portal Logon ID Password

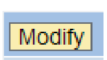
You can reset Portal user passwords in two cases:

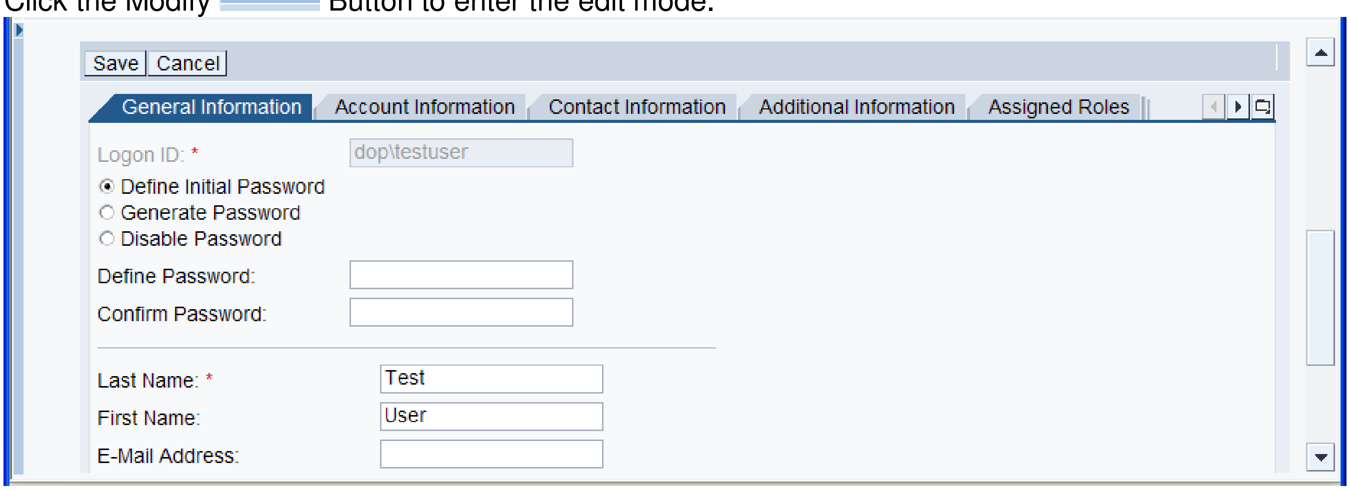
- ESS users (8 digit personnel number)
- NON SSO professional users (domain\username)

NOTE: *LDAP e-mail accounts' passwords are reset by your agency's Network Administrators this in turn will change the user's password to their PC.*
NOTE: *UME Professional and Personal ESS user account – if there is an email address in the email field of the account, the new initial password will be sent to the user after you reset it.*
NOTE: *When you are searching for an ESS User Portal account using the advanced search and no user comes up, try searching for their full 8-digit personnel number. The user might have changed their name, in that case you will have to update their name. If the user still does not come up in the search, contact the DOP Help Desk with the User's name and full 8-digit personnel number.*

1. Search for a user that needs his/her password reset either using the search box, or the Advanced Search option.
2. Click on the box to the left of the user to select it, the line will become highlighted.



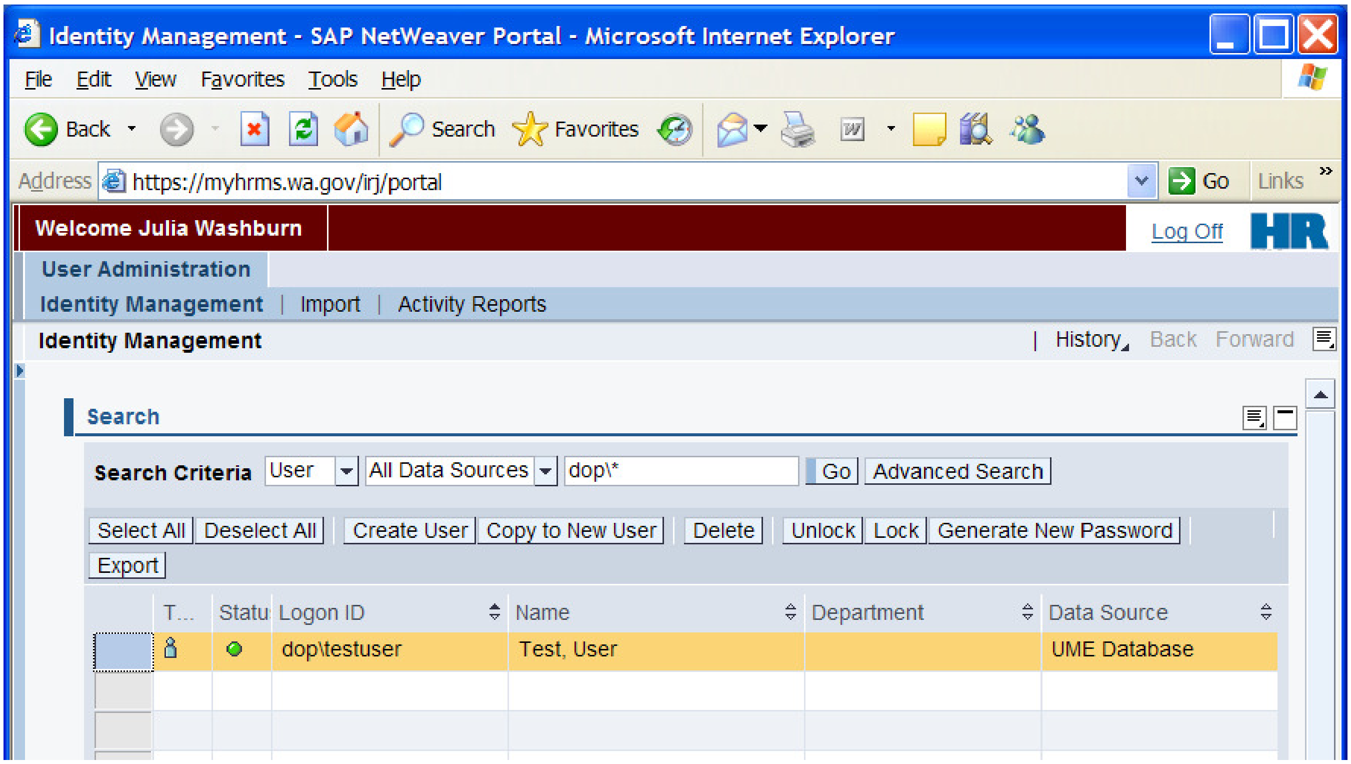
3. Click the Modify  Button to enter the edit mode.



4. Enter Define Password and Confirm Password
5. Click the Save button

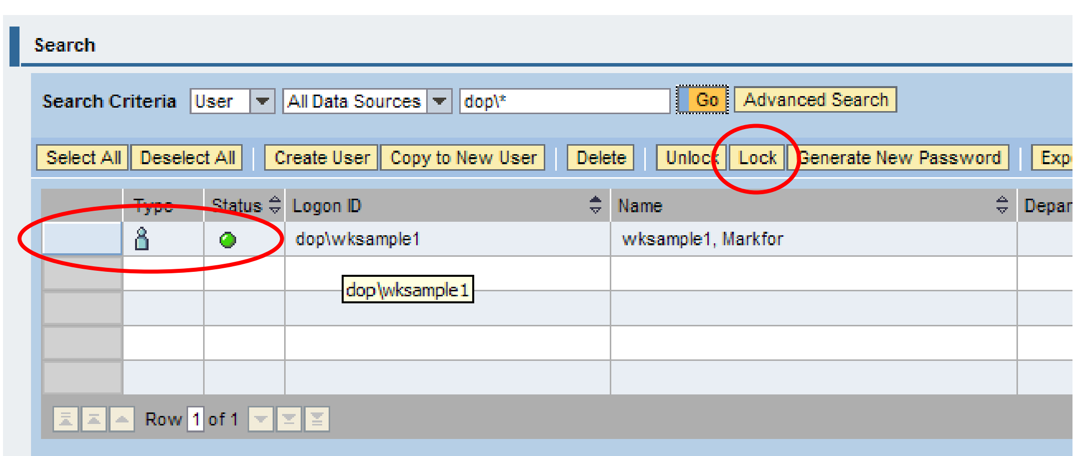
Lock/Unlock Portal Logon ID's

1. Logon to Portal; open your web browser and enter this URL: https://myhrms.wa.gov/irj or https://wahrms.wa.gov/irj.
2. Search for a user by either entering something in the search box (EX: dop*) or using the Advanced Search option.
3. Click the box to the left of the Logon ID to select the user.

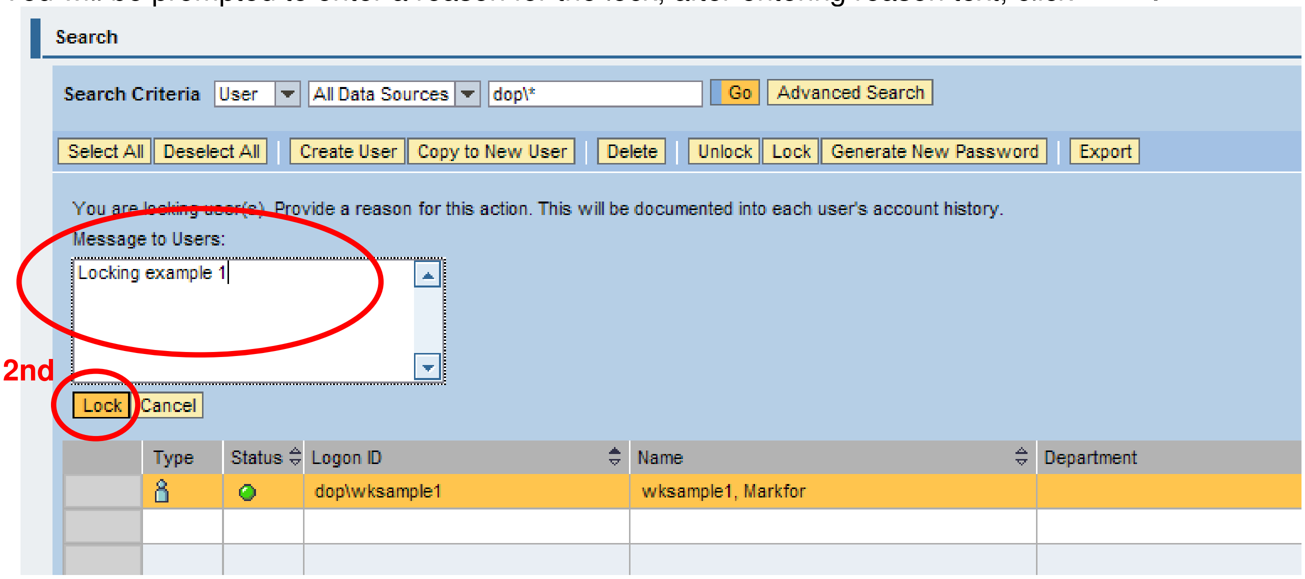


To LOCK a specific Portal Logon ID

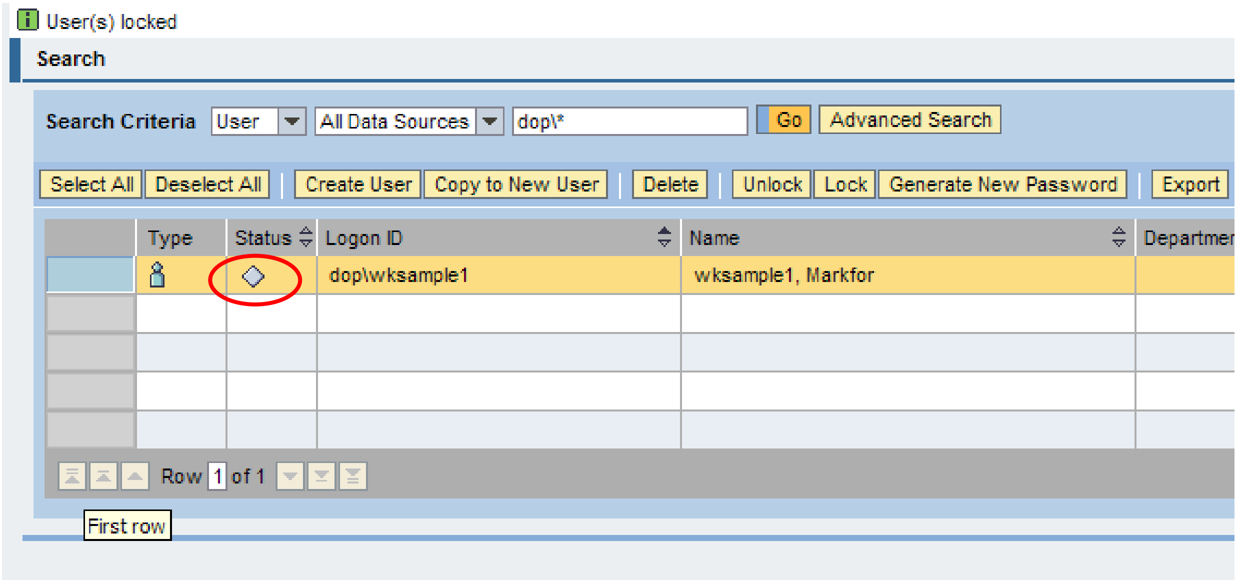
a. At the search response form, click on the selection box to the left of the desired user's name and click the "lock" button



b. You will be prompted to enter a reason for the lock, after entering reason text, click Lock.

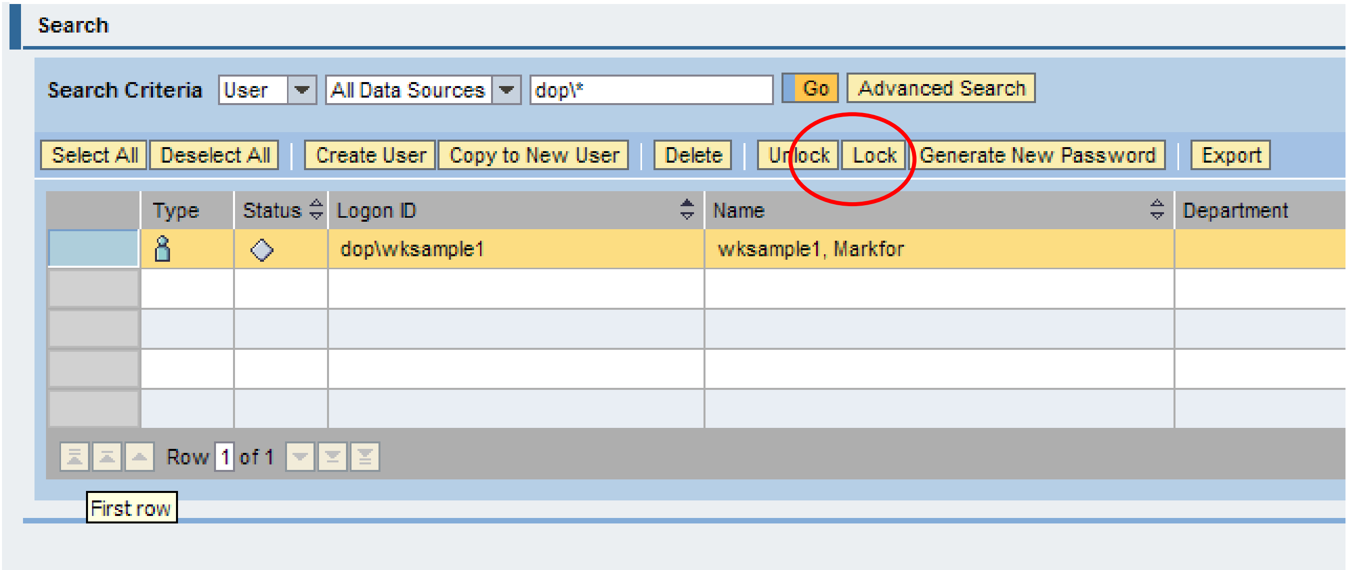


c. Upon successful lock, a message will appear and the user's Status Icon will change from Green Circle to a Blue Diamond.

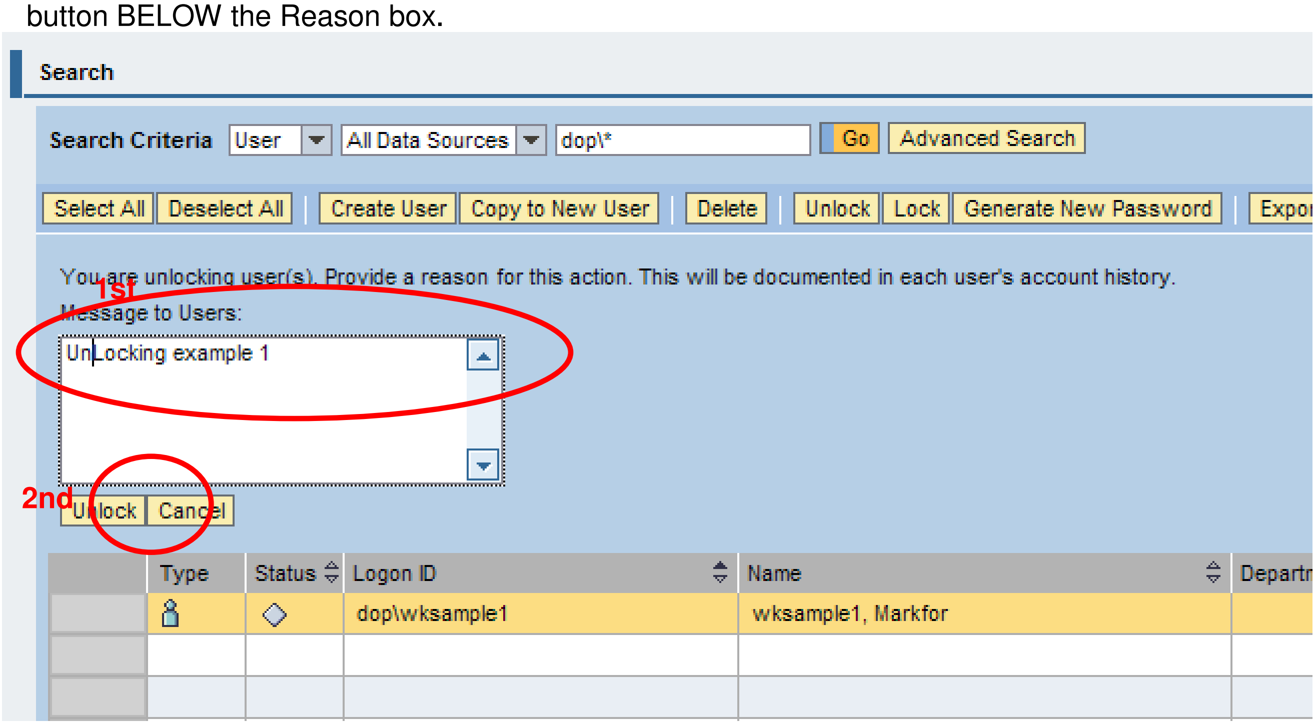


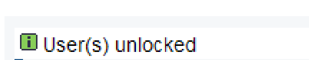
To UNLOCK a specific Portal Logon ID

d. Select the box to the left of the Portal Logon ID you want to unlock and click the Unlock button ABOVE the name.



e. You will be prompted to enter a reason for the unlock, after entering reason text, click the Unlock button BELOW the Reason box.



f. Upon successful unlock, a 

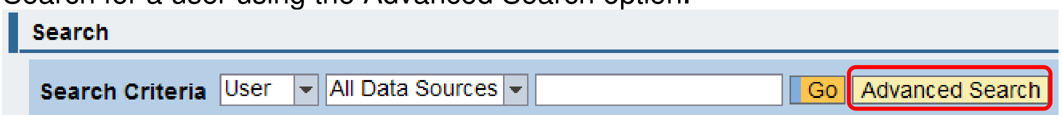
message will appear and the user's status icon will change to a green ball.

Delete PORTAL domain\username Accounts (UME)

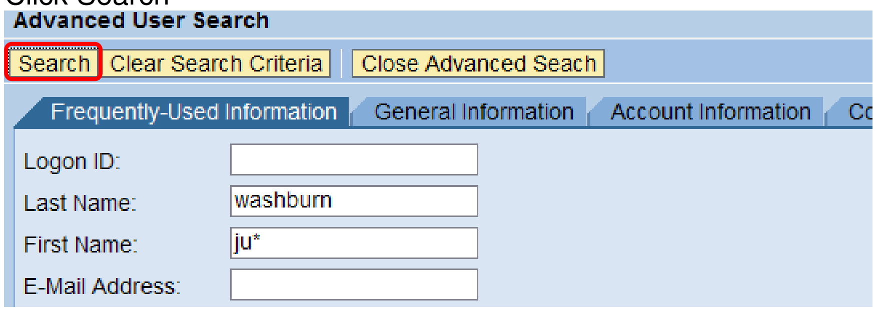
NOTE: *For the process when people leave your agency refer to [UserID Maintenance when Employees (ESS/Professional Users) Leave the Agency]()*

1. Logon to HRMS Portal; https://myhrms.wa.gov/irj or https://wahrms.wa.gov/irj.

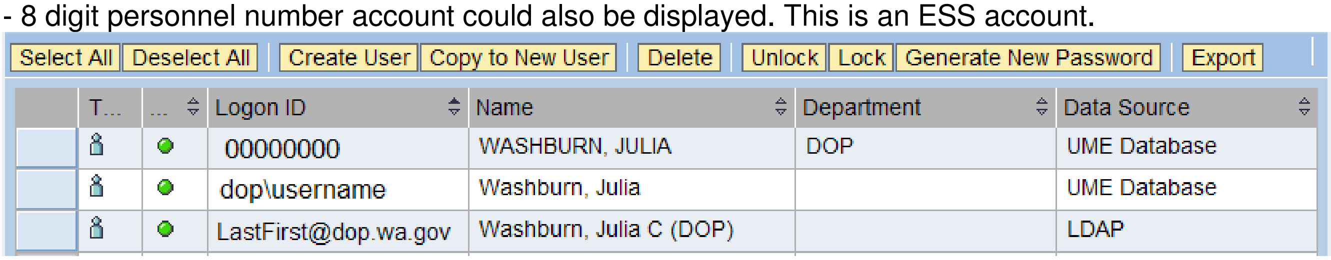
2. Search for a user using the Advanced Search option.



3. Enter Last Name and couple of letters of the first name with an *
4. Click Search

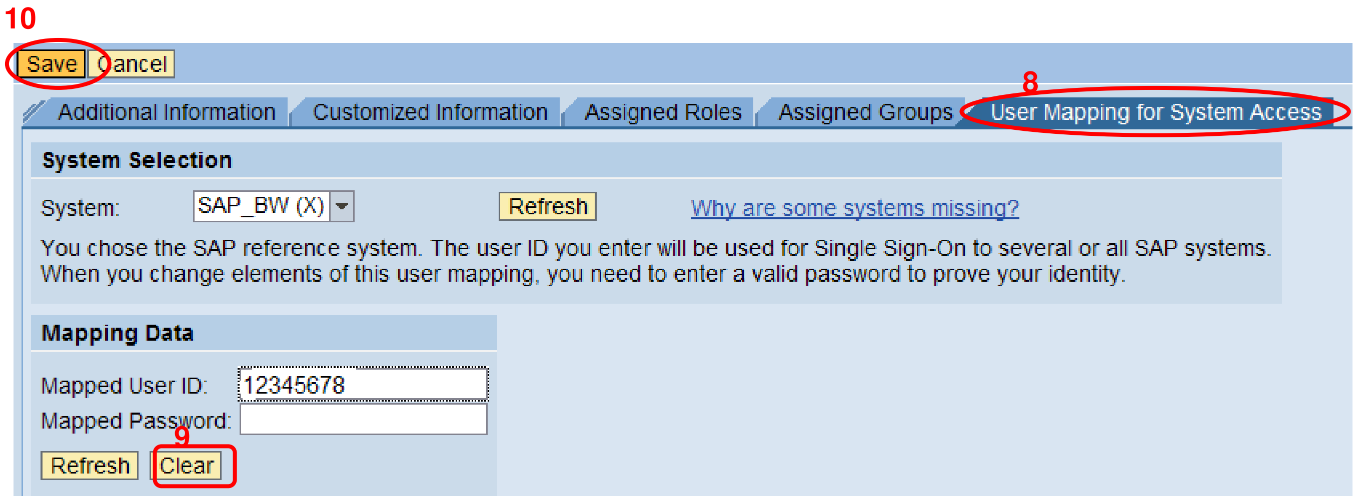


5. Users will be displayed in the table.
- If your agency is outside the SGN your professional user accounts will be your agency domain\username such as **dop\username** (UME)
- If your agency is inside the SGN your professional user accounts will be your agency e-mail address such as LastFirst@dop.wa.gov (LDAP).
- 8 digit personnel number account could also be displayed. This is an ESS account.

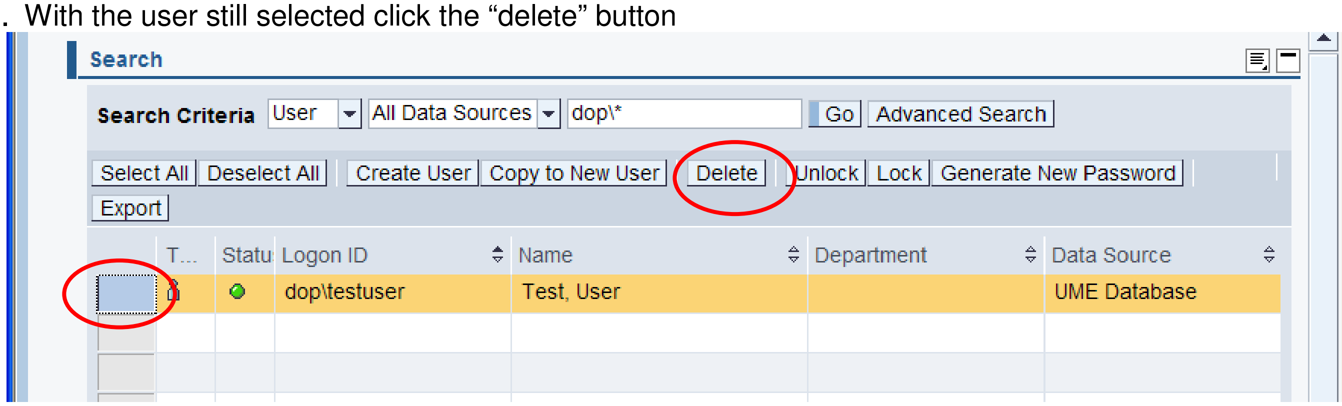


6. Click the box to the left of the Logon ID to select the user
7. Click the Modify button to enter the edit mode
8. Click the User Mapping for System Access
9. Click the Clear button to clear the mapping
***Effective April 26, 2010 you MUST also contact the DOP Service Center to have Professional Portal accounts mapping cleared from the Federated Portal. You will need to provide the BI UserID and current password and the Professional Portal account userID (LDAP or UME). Send requests to the DOP Service Center at servicecenter@dop.wa.gov or contact 360-664-6400.*

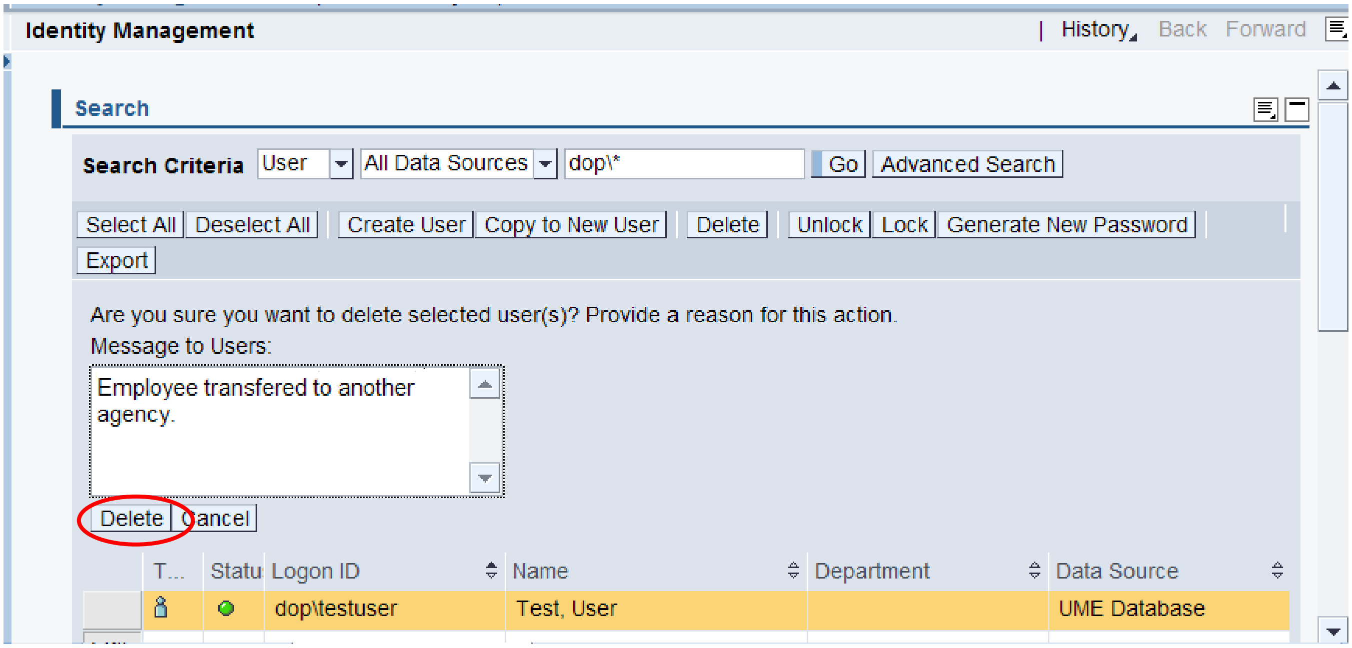
10. Click the Save button.



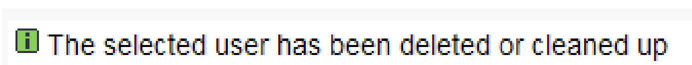
11. With the user still selected click the "delete" button



12. Enter the reason for the account deletion and click Delete button.



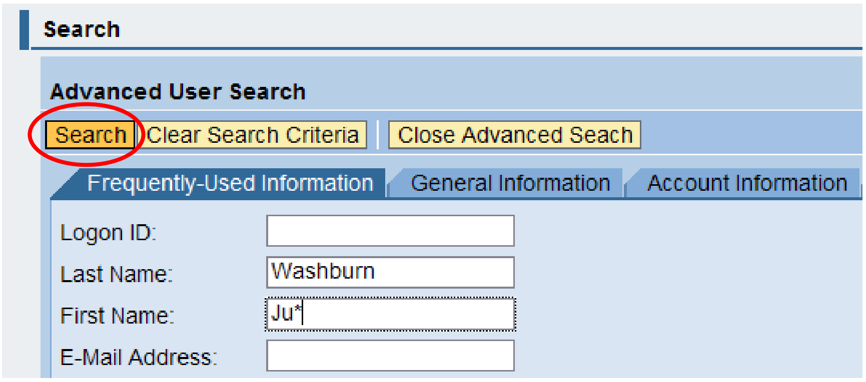
13. Upon successful deletion, the following message will appear at the top of the User List.



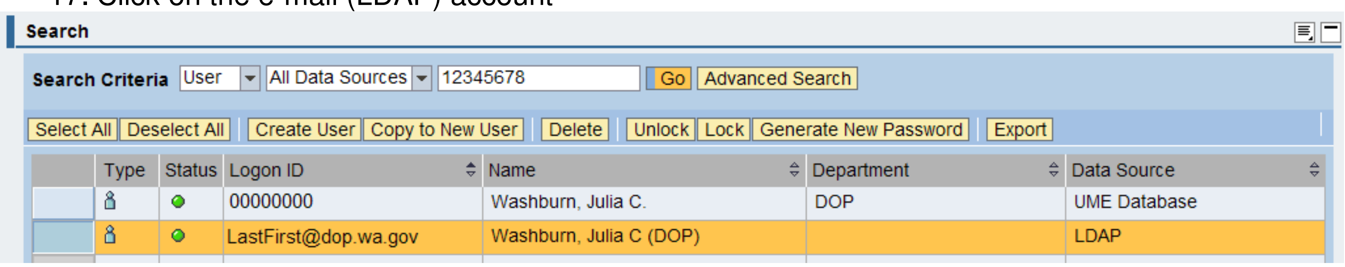
Delete Access from PORTAL E-Mail Account (LDAP)

NOTE: *You cannot delete an LDAP e-mail account.*

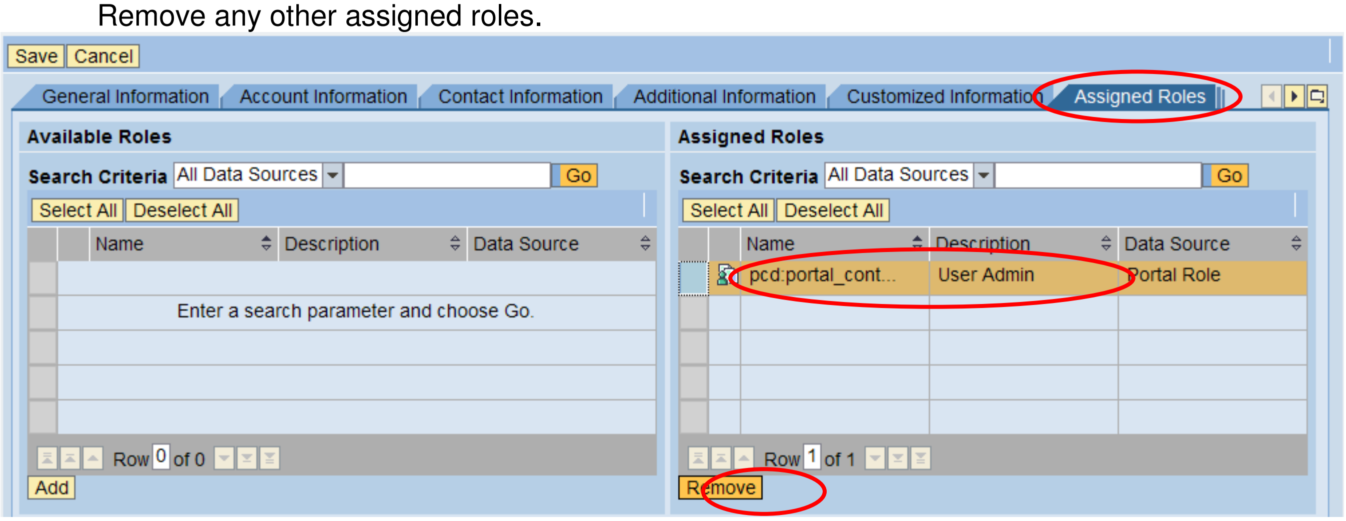
14. Logon to Portal; https://myhrms.wa.gov/irj or https://wahrms.wa.gov/irj.
15. Click the Advanced Search button
16. Enter the Last name and Couple of letters of the first name with an *, and click the Search button

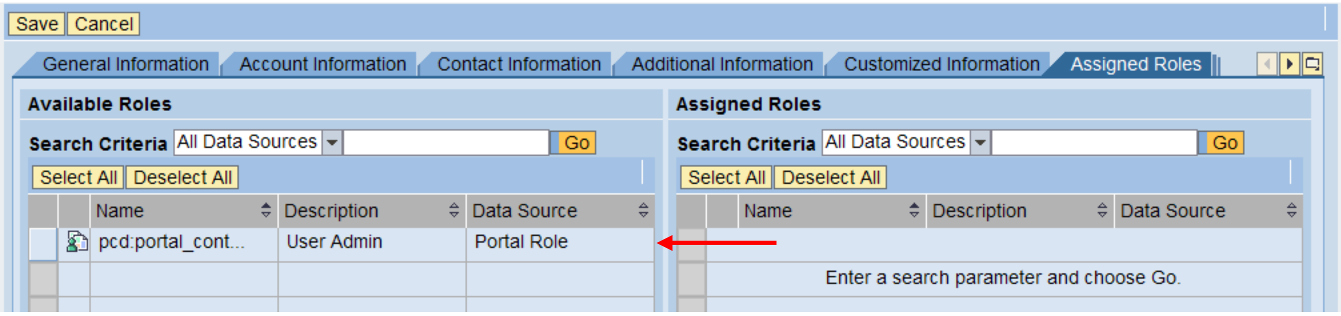


17. Click on the e-mail (LDAP) account

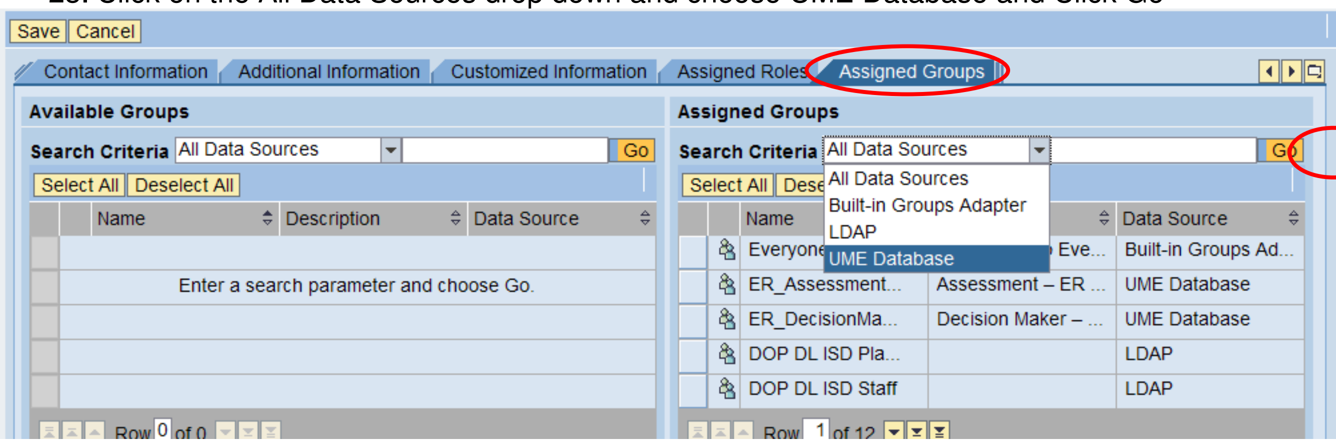


18. Click the Modify button to enter editing mode
19. Click the Assigned Roles tab. If there are any roles you need to delete them.
20. Click on the User Admin role
21. Click the Remove button; the removed role will be moved to the Available Roles section. Remove any other assigned roles.

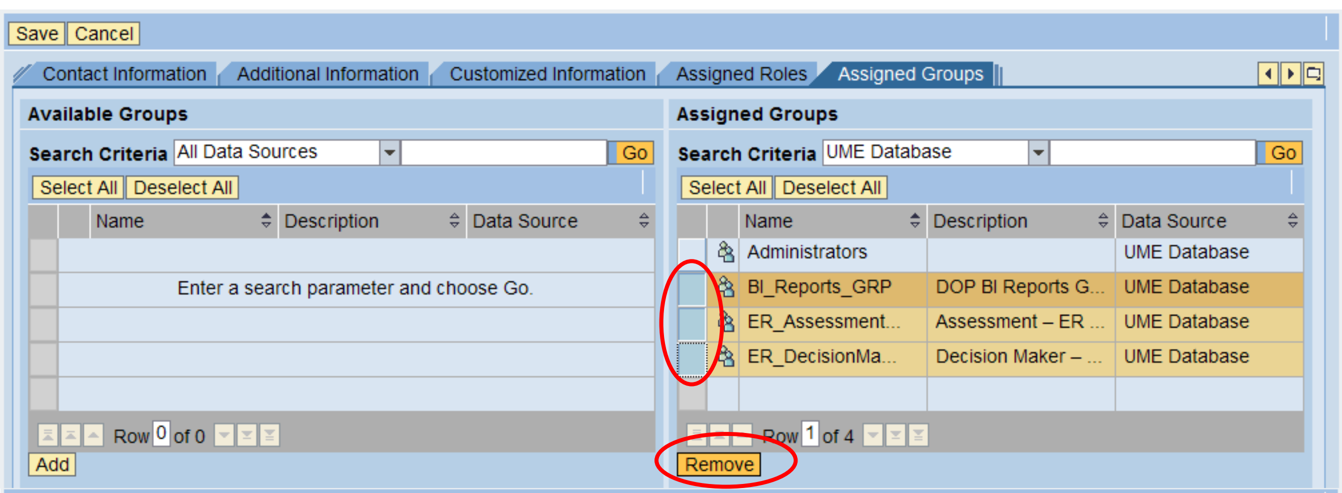


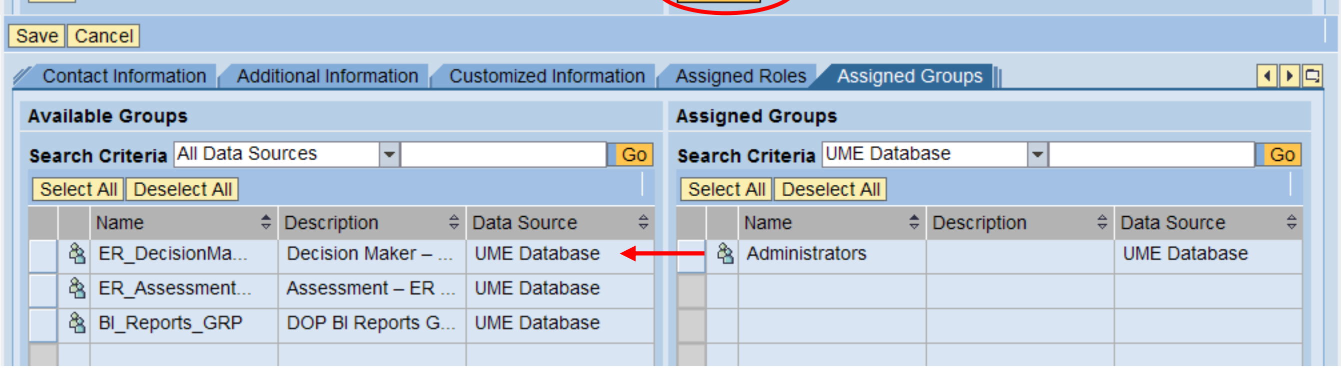


22. Click on the Assigned Groups tab
23. Click on the All Data Sources drop down and choose UME Database and Click Go



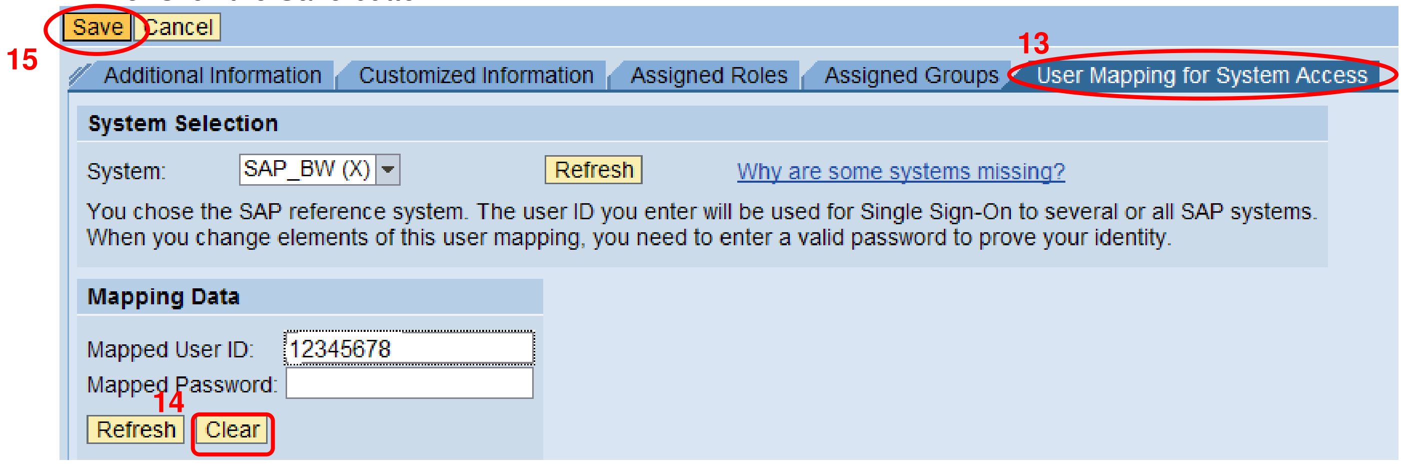
24. Click on the Group role
25. Click the Remove button; the removed Group Role(s) will be moved to the Available Groups section. Remove any remaining Group Roles.





26. Click the User Mapping for System Access
27. Click the Clear button to clear the mapping
    ***Effective April 26, 2010 you MUST also contact the DOP Service Center to have Professional Portal accounts mapping cleared from the Federated Portal. You will need to provide the BI UserID and current password and the Professional Portal account userID (LDAP or UME). Send requests to the DOP Service Center at servicecenter@dop.wa.gov or contact 360-664-6400.*

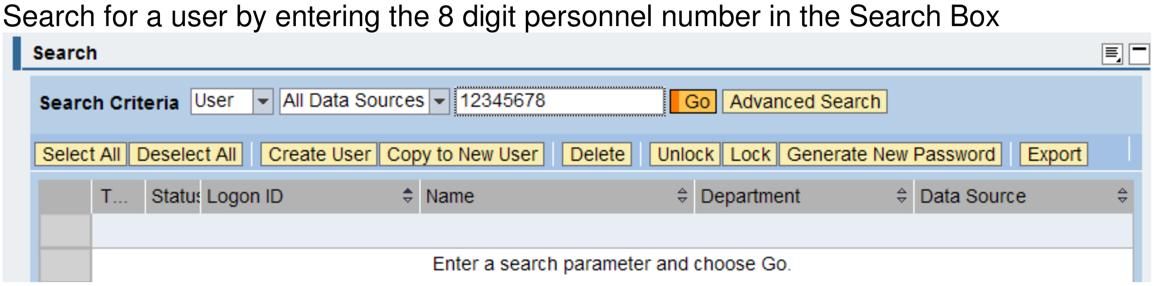
28. Click the Save button.



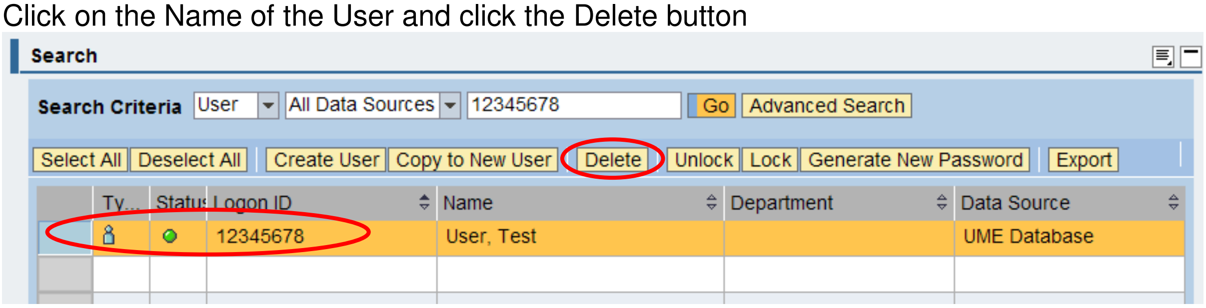
Non-Professional Users (ESS Users) Leave State Employment – Employee Status is Withdrawn:

<u>HRMS PORTAL:</u>

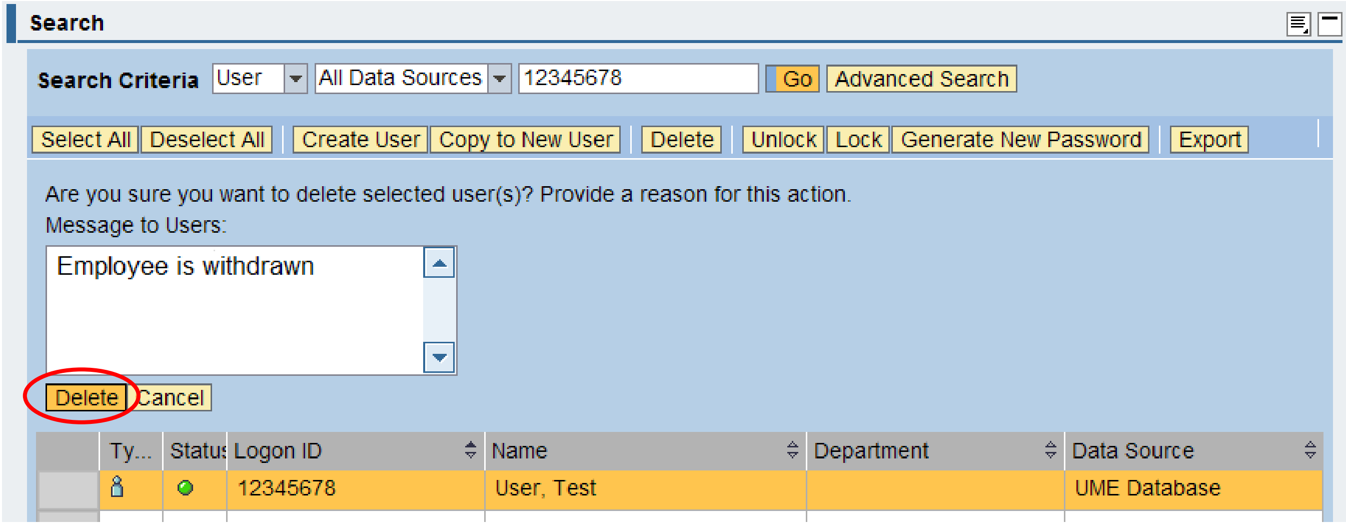
1. Logon to Portal; https://myhrms.wa.gov/irj or https://wahrms.wa.gov/irj
2. Search for a user by entering the 8 digit personnel number in the Search Box



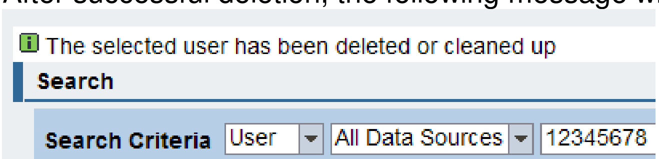
3. Click on the Name of the User and click the Delete button



4. Enter the reason for deletion and click the Delete button.



5. After successful deletion, the following message will be displayed.

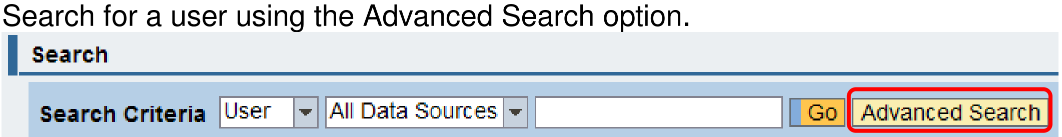


Professional Users Transfer out of the Agency or Professional Users Become Non-Professional Users (ESS Users):

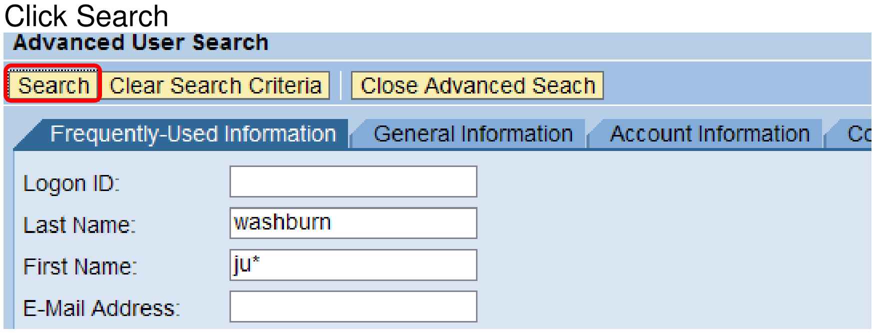
HRMS PORTAL domain\username UME account:

1. Logon to HRMS Portal; https://myhrms.wa.gov/irj or https://wahrms.wa.gov/irj.

2. Search for a user using the Advanced Search option.

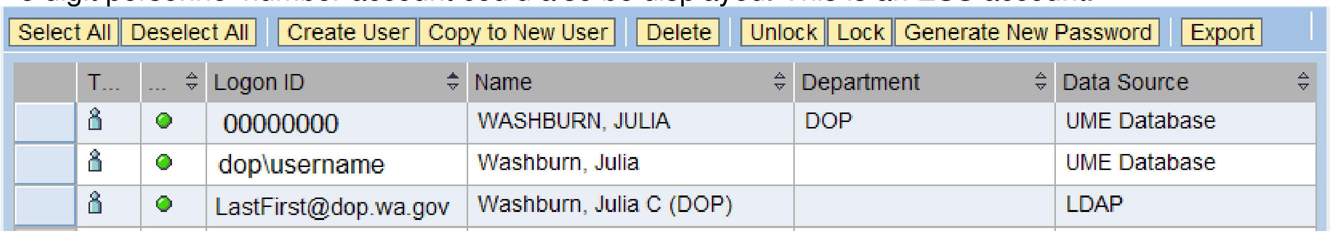


3. Enter Last Name and couple of letters of the first name with an *
4. Click Search

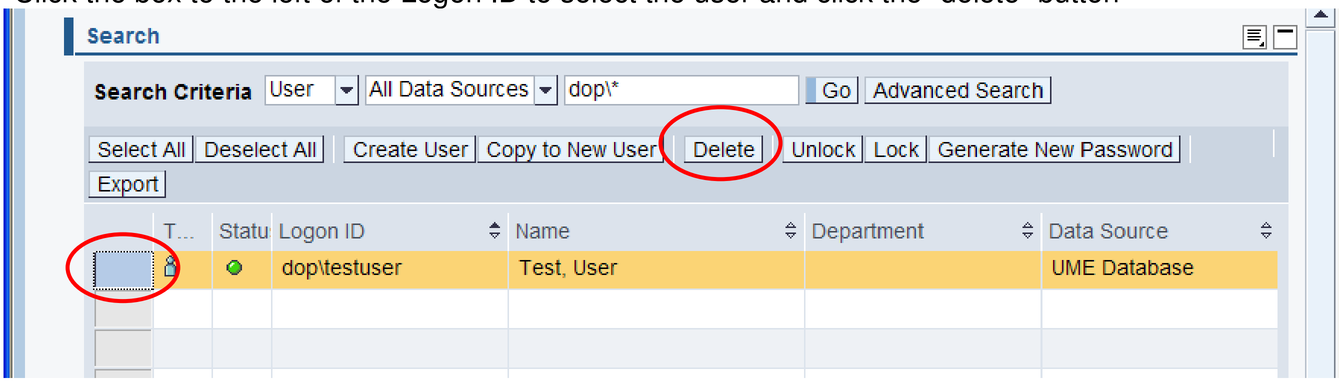


5. Users will be displayed in the table.
- If your agency is outside the SGN your professional user accounts will be your agency domain\username such as **dop\username** (UME)

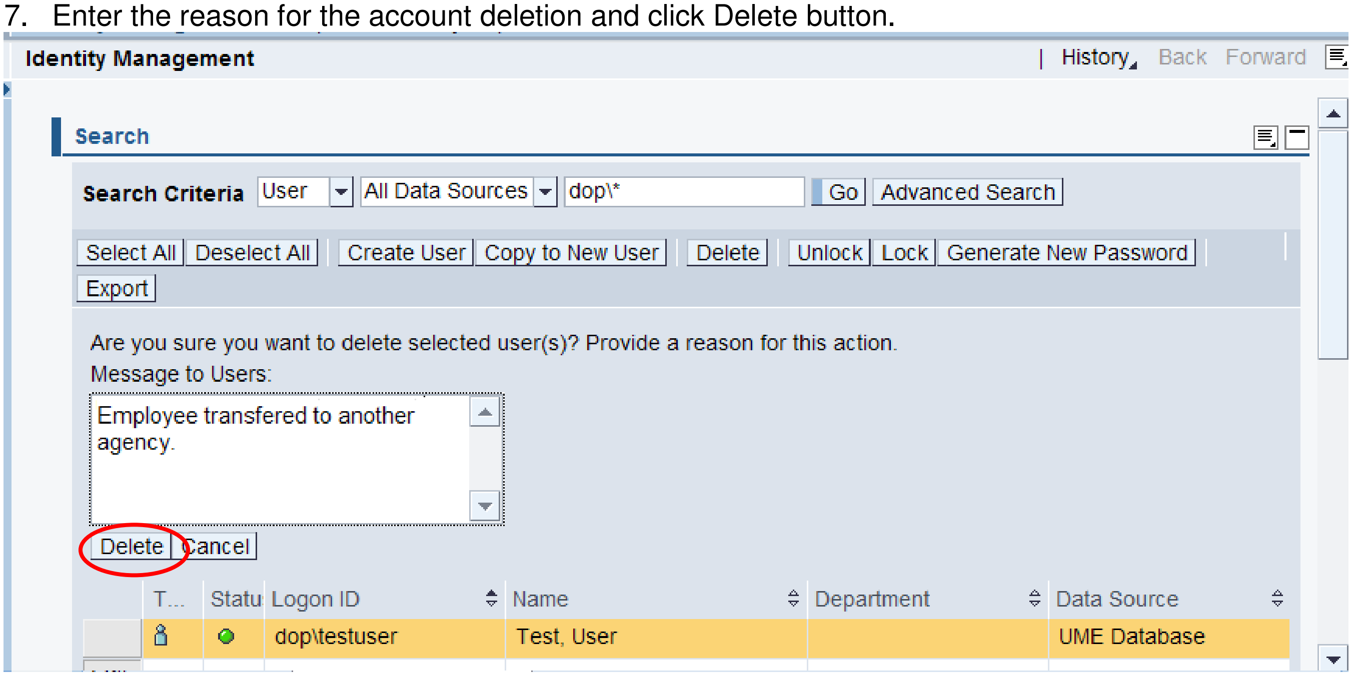
- If your agency is inside the SGN your professional user accounts will be your agency e-mail address such as LastFirst@dop.wa.gov (LDAP).
- 8 digit personnel number account could also be displayed. This is an ESS account.



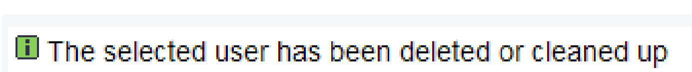
6. Click the box to the left of the Logon ID to select the user and click the “delete” button



7. Enter the reason for the account deletion and click Delete button.



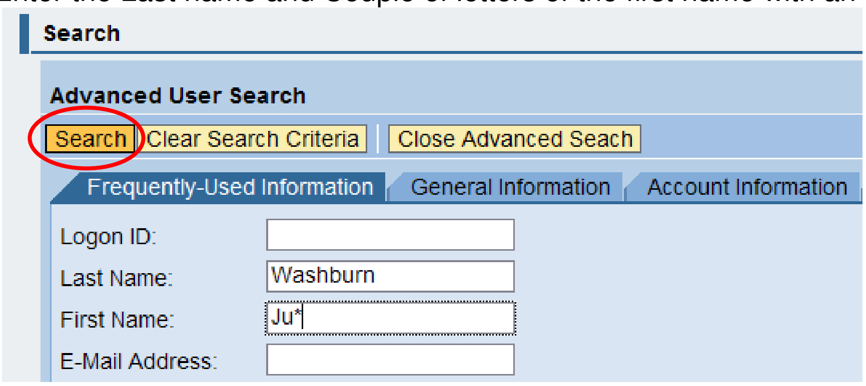
8. Upon successful deletion, the following message will appear at the top of the User List.



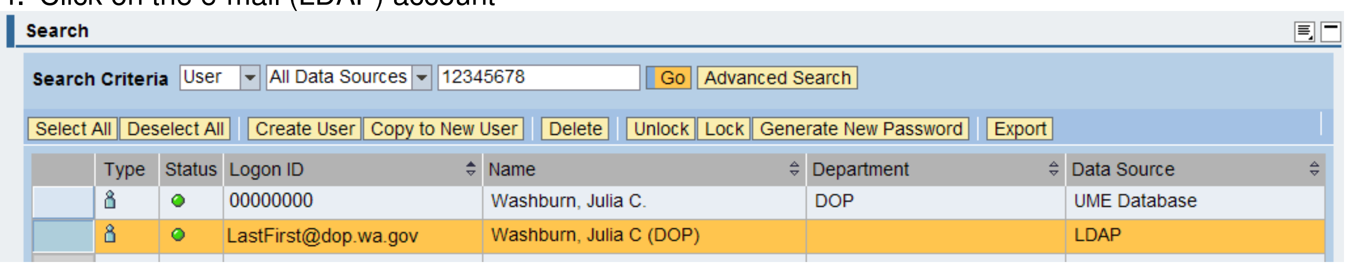
HRMS PORTAL e-mail LDAP account:

NOTE: *You cannot delete an LDAP e-mail account.*

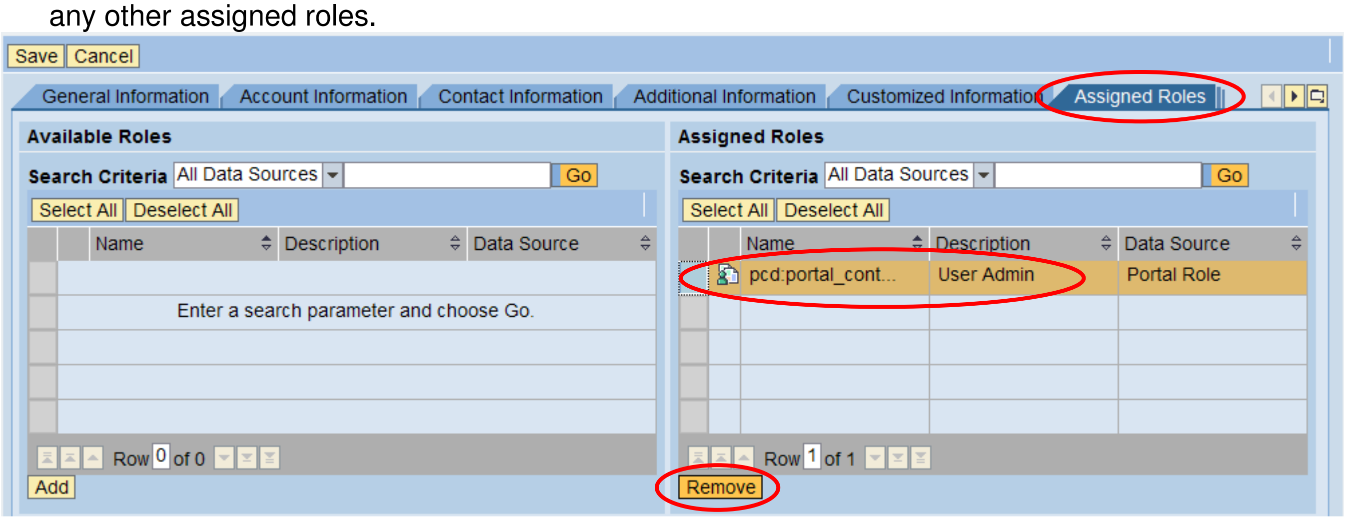
1. Logon to Portal; https://myhrms.wa.gov/irj or https://wahrms.wa.gov/irj.
2. Click the Advanced Search button
3. Enter the Last name and Couple of letters of the first name with an *, and click the Search button

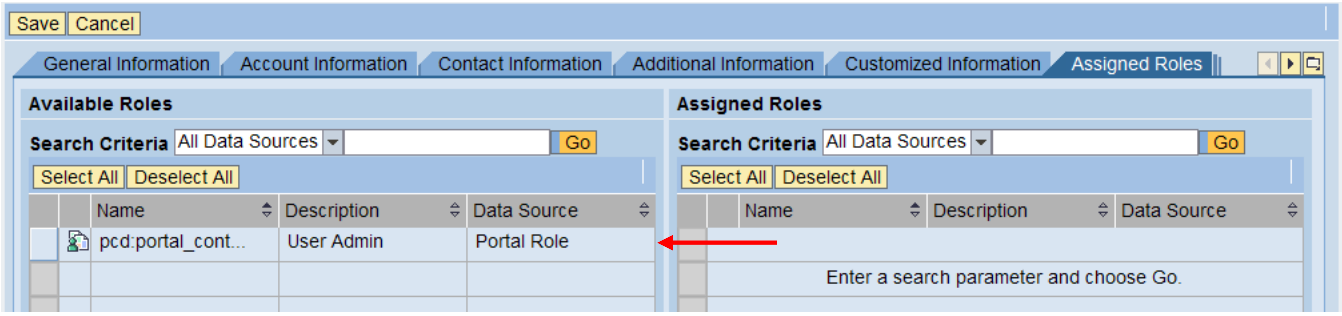


4. Click on the e-mail (LDAP) account

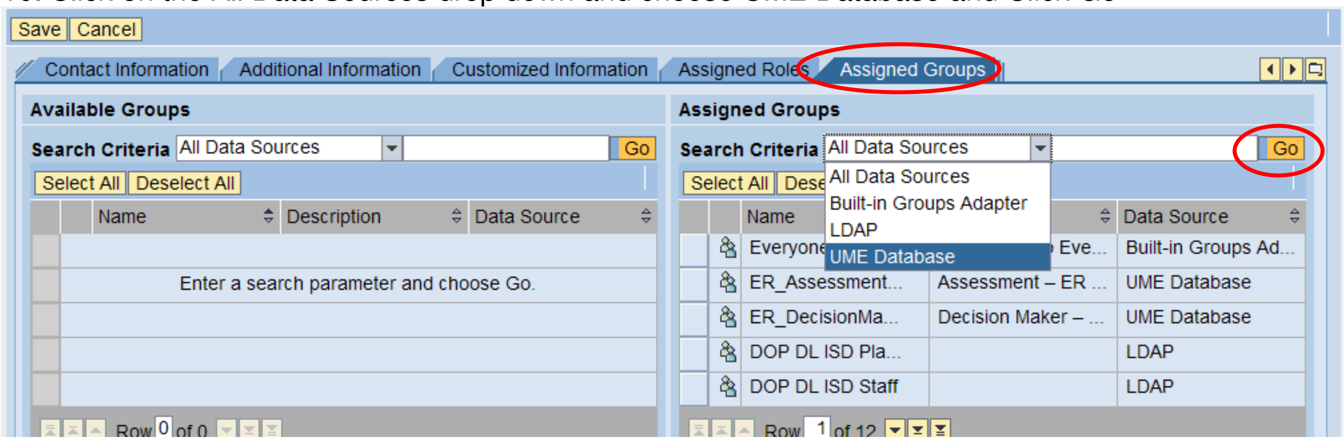


5. Click the Modify button to enter editing mode
6. Click the Assigned Roles tab. If there are any roles you need to delete them.
7. Click on the User Admin role
8. Click the Remove button; the removed role will be moved to the Available Roles section. Remove any other assigned roles.

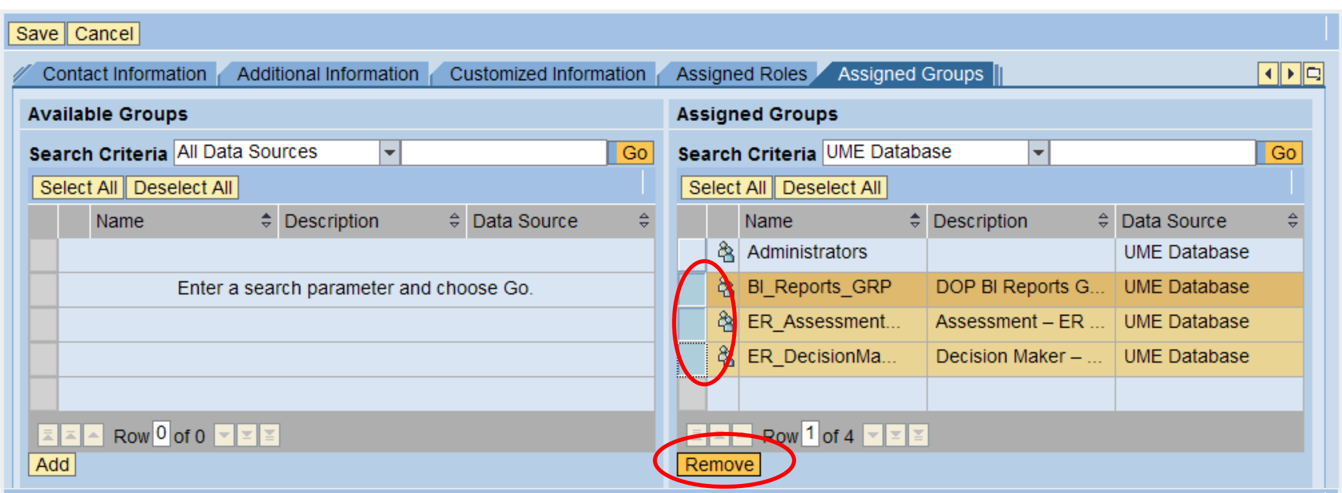


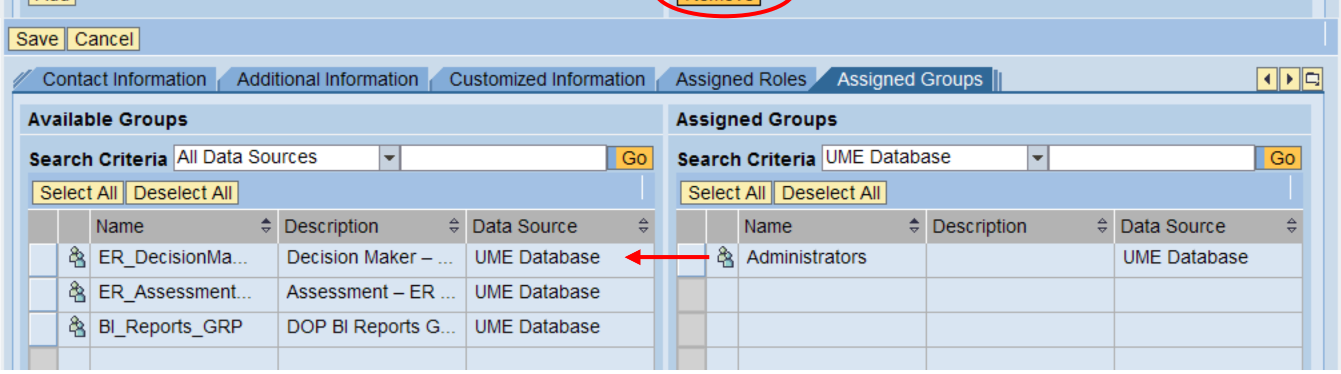


9. Click on the Assigned Groups tab
10. Click on the All Data Sources drop down and choose UME Database and Click Go



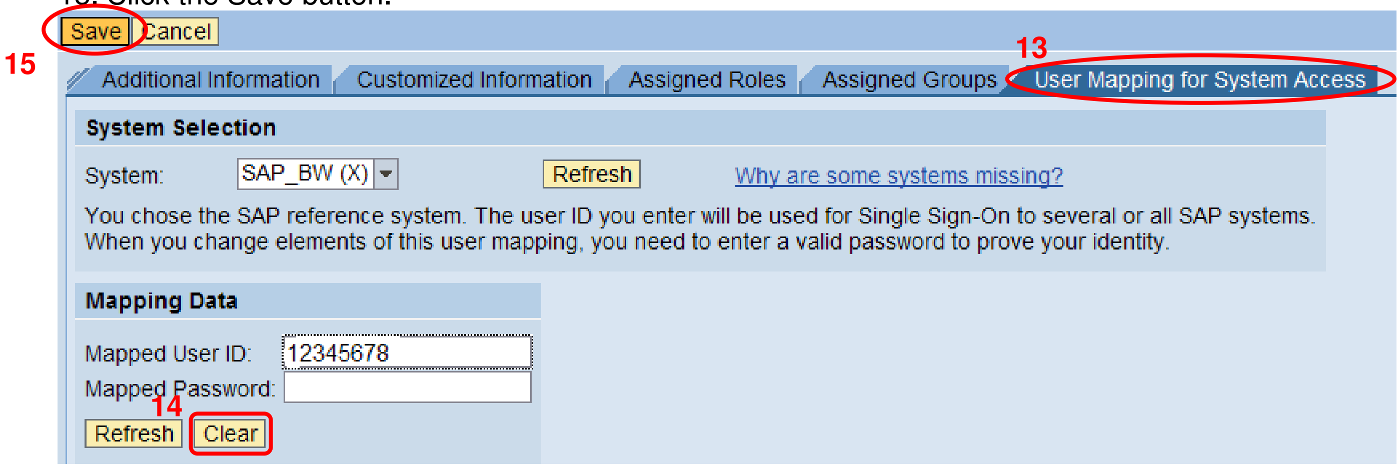
11. Click on the Group role
12. Click the Remove button; the removed Group Role(s) will be moved to the Available Groups section. Remove any remaining Group Roles.





13. Click the User Mapping for System Access
    14. Click the Clear button to clear the mapping
    ***Effective April 26, 2010 you MUST also contact the DOP Service Center to have Professional Portal accounts mapping cleared from the Federated Portal. You will need to provide the BI UserID and current password and the Professional Portal account userID (LDAP or UME). Send requests to the DOP Service Center at servicecenter@dop.wa.gov or contact 360-664-6400.*

15. Click the Save button.

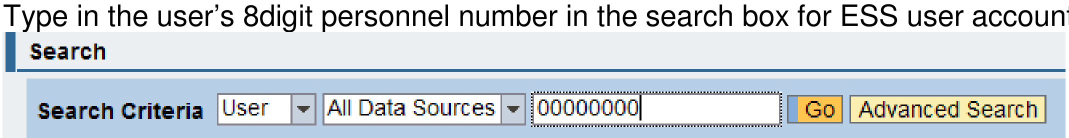


Employee has a Name Change

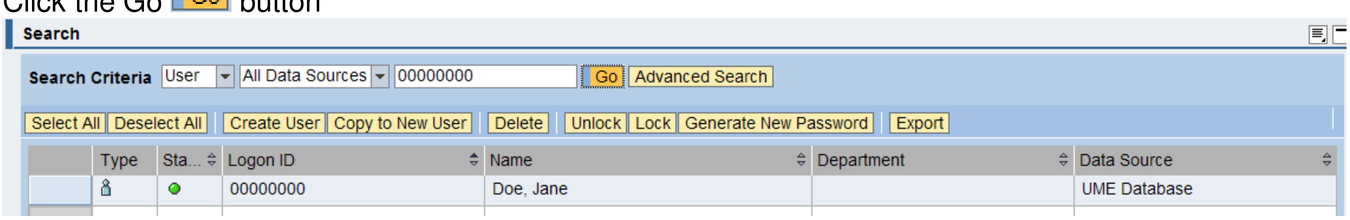
NOTE: *When an employee has a name change and the HCM personnel master record is updated, this change does not update the ESS User account (8 digit personnel number) or the UME professional account (domain/username) for that employee in the Portal. The Agency User Administrator must manually go into the Portal and change the employee's name on the ESS account, and recreate the Professional UME account with the new name and logonID.*

Changing the Name in the ESS or domain\username (UME) Portal Account

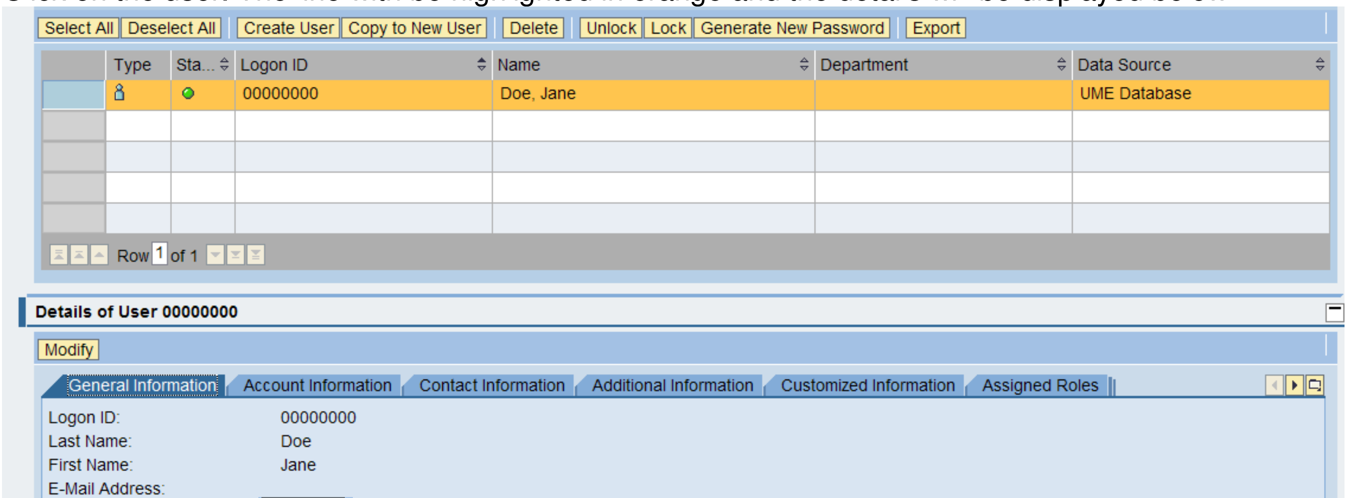
1. Logon to Portal; https://myhrms.wa.gov/irj or https://wahrms.wa.gov/irj
2. Type in the user's 8digit personnel number in the search box for ESS user account



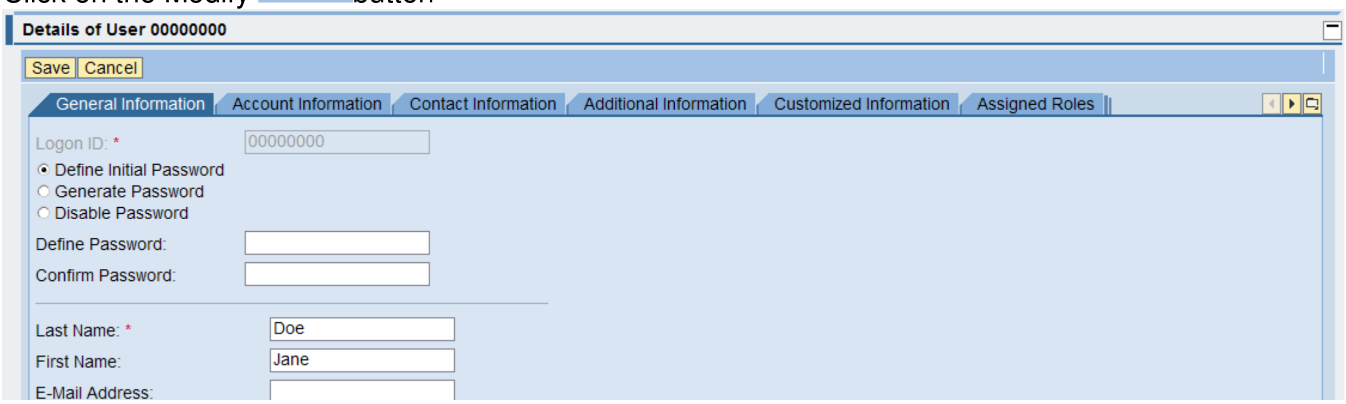
3. Click the Go Go button



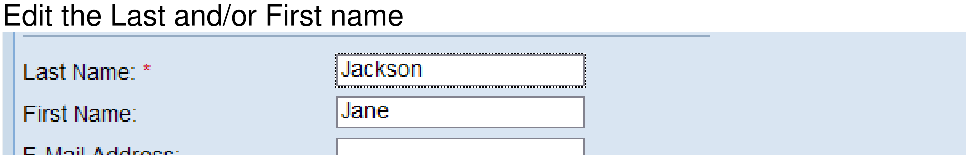
4. Click on the user. The line with be highlighted in orange and the details will be displayed below



5. Click on the Modify Modify button



6. Edit the Last and/or First name



7. Click Save Save

Changing the LogonID for the domain\username (UME) Portal Account

NOTE: *In order to change the LogonID in the UME Professional Portal account (domain\username) you will have to [create a new Professional Portal account]() assign roles/group roles, and map to BI. Then remove mapping from the old Professional Portal account with the old name and delete it..*